7

Technology, Nudges, Reputation, and Voluntary Compliance

INTRODUCTION

This chapter explores whether technology can be used to enhance noncoercive compliance by creating more effective reputational mechanisms and technological nudges. The discussion focuses on two main questions about technology usage. We first ask whether it is possible to monitor and enforce regulations while minimizing the impact of crowding out, at least as being subjectively perceived by the individual. The second question is whether technology can help identify which parts of the population can be trusted to comply voluntarily; a concept related to differentiated trust, as we have explored earlier in this book. It is important to note that, on the surface, the second goal may appear to resemble the Chinese social credit system (SCS) that seeks to exploit technology in order to enable the state to monitor and control people's social behavior (see the section "China's Social Credit System: Trustworthiness"). However, our focus on technology aims for quite a different situation, as we are looking for ways in which the state can become less coercive and more trusting toward more people.

Generally speaking, using technology to enhance compliance could lead to two developments. On the one hand, improved technological monitoring could reduce the need to rely on people's voluntary compliance. By providing clear instructions and analyzing behavioral patterns, this technology could complement research on personalization and technology-based enforcement.[1] This could potentially facilitate various types of cooperation among people, which could reduce or eliminate the need for state monitoring or the use of sanctions as part of a command-and-control approach.

[1] Porat, Ariel, and Lior Jacob Strahilevitz. "Personalizing default rules and disclosure with big data." *Michigan Law Review* 112 (2013): 1417–1478. Some workplaces use wearable wireless sensors that relay data to algorithms in order to emotionally monitor their employees. By tracking employees' emotional states, managers can analyze the effectiveness of company policies and procedures. In China, brain surveillance is conducted without consent. See Nelson, J. S. "Management culture and surveillance." *Seattle University Law Review* 43 (2019): 631–682.

https://doi.org/10.1017/9781009057998.008 Published online by Cambridge University Press

On the other hand, technology can help foster a more trusting relationship between citizens and the state, allowing officials to grant people greater discretion while avoiding direct monitoring of their activities. By using personalized data on past behavior, as discussed in the work with Aronson and Lobel on trust-based regulation, the state can achieve a balance between allowing greater freedom for more people without harming those who are less deserving of this trust.[2]

Research conducted in the field of algorithmic management has produced mixed results regarding the potential crowding-out effect of rating and monitoring procedures.[3] This poses a challenge to the idea that technology can enhance intrinsically motivated compliance, as these procedures may only minimally reduce the need for state-imposed sanctions. While it is true that technology can replace certain forms of enforcement, much of the current research suggests that it may also lead to alienation among people.[4] Therefore, in this chapter, we will examine the potential pitfalls of using technology as a substitute for state enforcement.

THE OVER-MONITORING DILEMMA

As noted, the primary challenge in using technology is determining whether we can achieve a high level of monitoring that renders the need to trust people unnecessary by enabling us to monitor nearly all actions individuals take. As we have argued, this new ability of the state could have divergent implications. It could either lead toward perfect monitoring, which would eliminate the need for trust, or it could allow the state to have faith in individuals whose past actions have been proven trustworthy. At the same time, in our normative analysis, we need to acknowledge that there is no such thing as perfect technological monitoring, at least not yet. This due to several aspects: First, people are not being monitored all the time; and second, there are instances where strict compliance is essential, but monitoring compliance can prove to be challenging for the state without violating privacy rights. For example, in the context of COVID, even the states that allowed themselves to use rather intrusive technology, such as contact tracing, could not monitor how people behaved in their own homes, where much of the virus's spread occurred.[5] Therefore, the state found it easier to monitor areas where voluntary compliance posed less of a problem, as it was epidemiologically less risky (e.g., open-air public

[2] Feldman, Yuval, Orly Lobel, and Ori Aronson. "The behavioral challenges of trust-based regulation: Navigating the complexities of past behavior as a predictor." Available at SSRN 5117987 (2025). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5117987.

[3] Dickinson, David, and Marie-Claire Villeval. "Does monitoring decrease work effort? The complementarity between agency and crowding-out theories." *Games and Economic Behavior* 63.1 (2008): 56–76.

[4] Rowe, Frantz, Ojelanki Ngwenyama, and Jean-Loup Richet. "Contact-tracing apps and alienation in the age of COVID-19." *European Journal of Information Systems* 29.5 (2020): 545–562.

[5] See, for example, www.ox.ac.uk/news/2020–09–03-new-research-shows-tracing-apps-can-save-lives-all-levels-uptake; www.bundesregierung.de/breg-de/themen/corona-warn-app/corona-warn-app-englisch.

https://doi.org/10.1017/9781009057998.008 Published online by Cambridge University Press

spaces). It was much more difficult for the state to enforce COVID regulations in closed spaces where more of the virus transfer could happen.[6] The need for voluntary compliance is especially important in areas where enforcement, especially technological enforcement, is most difficult.

One of the concerns we have about voluntary compliance is related to the need to convince people who are not initially supportive of the government's policy to act in a trustworthy manner. This process may undermine people's autonomy and it should be compared to the negative impact that algorithmic regulation can have on autonomy. Therefore, the comparison between the two approaches should focus on which approach is more detrimental to people's freedom of choice in deciding whether to comply with state laws and regulations. The comparison becomes even more complex when considering the role of technology, including big data approaches, in identifying people who may not need convincing, as their behavior should influence the decision between a technology-based approach and a trust-based approach. For those individuals, regulations based on trust – a concept that was explained in more detail in Chapter 4 – do not require any internalization process. Therefore, such people may find the use of technology far less desirable.

In this chapter, we will explore several critical aspects of the interaction between technology and voluntary compliance. Technology fundamentally shapes the relationship between citizens and government, sometimes constraining human decision-making flexibility. In traditional human-mediated interactions, inconsistent treatment based on personal characteristics may be more prevalent and harder to trace compared to technological solutions.

The advancement of technological enforcement capabilities has paradoxically increased the importance of voluntary compliance, while simultaneously enabling governments to differentiate their approach based on individuals' compliance histories. This development aligns with a broader trend toward personalized regulation, where technological solutions facilitate more individualized regulatory approaches that better align with personal preferences and circumstances.

Furthermore, technological progress has enhanced the ability to design and implement sophisticated incentive systems, creating new pathways for encouraging voluntary compliance. These technological innovations in incentive design may foster the long-term internalization of compliant behavior, potentially transforming temporary compliance into sustained voluntary cooperation. The combination of improved enforcement capabilities, personalization, and sophisticated incentive systems creates new opportunities for promoting and sustaining voluntary compliance while addressing traditional challenges in regulatory implementation.

[6] For the general problem of enforcement focusing on the wrong place, see Feldman, Yuval, and Yotam Kaplan. "Ethical blind spots and regulatory traps: On distorted regulatory incentives, behavioral ethics & legal design." In *Law and economics of regulation*, edited by Klaus Mathis and Avishalom Tor, Springer International Publishing, 2021: 37–54.

https://doi.org/10.1017/9781009057998.008 Published online by Cambridge University Press

TECH-ENABLED CIVIC ENGAGEMENT

Extensive research in the intersection of technology and governance has focused on e-government, a relatively new mode of citizen-to-government contact that takes advantage of information and communications technologies. Similarly, Im and colleagues (2014)[7] investigated the impact of internet use on government trust and citizen compliance in South Korea. They found that increased internet use led to decreased trust and compliance, but e-government programs could effectively counter these problems.

The success of e-government is based on governments' trust in their citizens and on how citizens view the government in terms of their technological experience when working with the government.[8] Findings suggest that although e-government may help improve citizens' confidence in an agency's future performance, it does not necessarily result in greater satisfaction with interaction with an agency, nor does it correlate with greater overall trust in the federal government.[9] To the best of our knowledge, most current research in these areas focuses on ethical issues related to the technological monitoring of citizens as well as the extent to which citizens are satisfied with the more efficient technological services being offered by governments.[10]

TECHNOLOGY: MORE MONITORING, LESS TRUST?

In many ways, the combined role of law and technology revolves around questions of differentiated trust and people's ability to trust technology. On one hand, as mentioned in the introduction to this chapter, technology is likely to reduce the incentive for people to cheat, ultimately resulting in reduced reliance on the government to trust in people's compliance.[11] A classic example of how technology improves monitoring is using cash. From a tax evasion standpoint, the cash economy is the most difficult to monitor. Several methods are being utilized to replace cash with more traceable alternatives, although this does not consider

[7] Im, Tobin, et al. "Internet, trust in government, and citizen compliance." *Journal of Public Administration Research and Theory* 24.3 (2014): 741–763.

[8] Welch, Eric W., Charles C. Hinnant, and M. Jae Moon. "Linking citizen satisfaction with e-government and trust in government." *Journal of Public Administration Research and Theory* 15.3 (2005): 371–391.

[9] Morgeson III, Forrest V., David VanAmburg, and Sunil Mithas. "Misplaced trust? Exploring the structure of the e-government–citizen trust relationship." *Journal of Public Administration Research and Theory* 21.2 (2011): 257–283.

[10] Asgarkhani, Mehdi. "The effectiveness of e-service in local government: A case study." *Electronic Journal of e-Government* 3.4 (2005): 157–166.

[11] Bamberger, Kenneth A. "Technologies of compliance: Risk and regulation in a digital age." *Texas Law Review* 88 (2010): 669–739.

https://doi.org/10.1017/9781009057998.008 Published online by Cambridge University Press

newer advancements such as Bitcoin, which are even more challenging to monitor by authorities.

As another example, compared to traditional taxi drivers those who work for Uber or other ridesharing apps are less likely to commit tax fraud when their earnings are received through the app.[12] Similarly, renting through booking websites like Airbnb is less likely to be vulnerable to tax evasion.[13] Furthermore, services like Airbnb, Uber, and Lyft not only help to reduce tax evasion but also offer ways for the public to determine whom they can trust based on social reputation and social-reporting systems.[14] For one, Alm's study examines the effects of technological progress on tax avoidance and evasion.[15] This work looks at these effects on individual taxpayers and the state, and it finds that technology has two effects: the first is that it increases the amount of information taken in by the government which makes tax evasion more difficult as the state can better combat tax evasion. While this means that most taxpayers will evade taxes less, this paper argues that technology also allows for a small group of taxpayers to more easily avoid taxes. This paper correlates wealth with the ability to do this, which means that in a more unequal society the wealthy can more easily avoid taxation.

SMART MONITORING REDUCES ENFORCEMENT

The goal of technology is to simplify the process by which states can have confidence in people, not necessarily because they inherently trust them, but because an algorithm suggests that less strict enforcement may be appropriate due to the fact that everything is being recorded. With the various privacy concerns, can we reduce the negative effects of technological surveillance? Can we raise the threshold for minor offenses so that they can be more easily overlooked? For example, the noncash shift may change the need for trust in taxation, as people might have harder time evading taxation, not to mention the even more dramatic blockchain revolution.[16] Similarly, we must ask ourselves if we are better off with contact-tracing apps than with epidemiological interviews with people who got infected?[17]

[12] https://morganjones.co.uk/2022/09/22/tax-dodging-taxi-drivers/.

[13] Alm, James. "Tax evasion, technology, and inequality." *Economics of Governance* 22.4 (2021): 321–343.

[14] Hawlitschek, Florian, Benedikt Notheisen, and Timm Teubner. "The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy." *Electronic Commerce Research and Applications* 29 (2018): 50–63.

[15] Alm. "Tax evasion, technology, and inequality."

[16] Mohanta, Bhabendu Kumar, Soumyashree S. Panda, and Debasish Jena. "An overview of smart contract and use cases in blockchain technology." In *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, IEEE, 2018: 1–4.

[17] Daisuke, Takagi, Amemiya Mamoru, and Shimada Takahito. "What do security cameras provide for society? The influence of cameras in public spaces in Japan on perceived neighborhood cohesion and trust." *Journal of Experimental Criminology* 18.1 (2022): 129–147.

https://doi.org/10.1017/9781009057998.008 Published online by Cambridge University Press

REGULATING SITUATIONS VS. REGULATING PEOPLE

The recent s-frame paper by Nick Chapter and George Lowenstein supports the view that technological advancements may reduce the need to change intrinsic motivation.[18] When discussing corporate climate change responsibility, the authors advocate prioritizing technologies that reduce the burden on individuals to address environmental challenges. Digital technologies could potentially replace traditional trust-based compliance mechanisms. With enhanced technological enforcement capabilities, governments may be able to move beyond questions of trustworthiness and focus instead on improving the quality of compliance outcomes, as explored in Chapter 1.

PROPORTIONALITY AND BEHAVIORAL BIG DATA

In a work in progress with Ori Aronson and Orly Lobel,[19] we study the concept of differentiated trust – a concept related to using people's past behavior – to decide whether trust-based regulatory attempts will be successful. In that paper, we analyze whether it's constitutional to treat people differently based on how their group has behaved in the past, rather than looking at their individual track record. This raises important questions about using group-level data to make trust-based decisions about individuals. We also examined how AI-powered data analytics can transform regulatory approaches to assessing individual and group trustworthiness. While traditional regulatory systems often rely on information concealment to protect privacy and equality, we propose that advanced algorithmic capabilities offer a new paradigm.

This new approach, sometimes called "fairness through awareness," leverages AI's sophisticated pattern recognition to process multiple data points while still protecting individual privacy. However, this capability raises important ethical questions: How do we ensure these systems promote genuine fairness rather than amplifying existing biases? How do we manage the risks of privacy breaches and discriminatory outcomes?

A key example is the use of machine learning to create individual "compliance scores" by aggregating various behavioral indicators. These scores typically evaluate factors such as accuracy of reporting, legal compliance, and ethical conduct. While such comprehensive profiling could enhance regulatory effectiveness, it also raises significant social and ethical concerns. For instance, how might minor norm violations affect an individual's overall trustworthiness assessment? And how do we ensure these scoring systems remain transparent and accountable?

[18] Chater, Nick, and George Loewenstein. "The i-frame and the s-frame: How focusing on individual-level solutions has led behavioral public policy astray." *Behavioral and Brain Sciences* 46 (2023): 1–26.

[19] Feldman, Lobel, and Aronson. "The behavioral challenges of trust-based regulation."

https://doi.org/10.1017/9781009057998.008 Published online by Cambridge University Press

Group-level trust assessments analyze patterns between regulatory compliance and group characteristics. While this data-driven approach aims for objectivity, it presents serious ethical challenges. Historical biases in data collection and interpretation could lead to discriminatory outcomes. For example, if past enforcement disproportionately targeted certain communities, these patterns might be incorrectly interpreted as reflecting inherent compliance differences. Moreover, automated systems might amplify existing socioeconomic disparities by applying stricter scrutiny to already disadvantaged groups, creating a self-reinforcing cycle of distrust. In my work with Kaplan,[20] we addressed an important gap in big data research – its potential role in regulatory decision-making. We examined how big data analytics could help identify trustworthy individuals in trust-based regulatory systems, using the COVID-19 pandemic as a key example. During the pandemic's early stages, governments needed to assess whether the public would voluntarily follow safety protocols rather than requiring strict enforcement.

Big data analysis offers unprecedented capabilities to differentiate between individual and group behaviors, enhancing our ability to predict voluntary compliance in trust-based regulatory systems. This predictive power becomes especially valuable in regulatory approaches that rely less on coercion and more on cooperation. Trust relationships are inherently reciprocal – when regulators demonstrate trust in the public, individuals often respond with increased trustworthy behavior. While this reciprocal dynamic is widely recognized, the empirical evidence examining how suspicion affects individual behavior remains limited.

This section examines the ethical dimensions of using data-driven approaches to regulate trust. Our analysis focuses on how differentiated regulatory strategies, based on data analytics, raise fundamental ethical questions.

Several key considerations emerge: First, how should we interpret and act upon statistical measures of trust? Second, what threshold of statistical significance justifies policy interventions? Third, what level of correlation between data points should be required before implementing differential treatment?

The justification for using predictive analytics varies by policy context. For instance, stronger privacy intrusions might be warranted for national security purposes than for improving tax collection efficiency. This aligns with the constitutional proportionality doctrine, which permits greater infringement on individual rights when pursuing objectives of higher public importance.[21]

Overall, the differentiated trust work in progress with Aronson and Lobel highlights the key ethical concerns related to differentiated lawmaking and regulation, particularly concerning trust regulation based on data. In our data-driven world, policymakers

[20] Feldman, Yuval, and Yotam Kaplan. "Big data and bounded ethicality." *Cornell Journal of Law and Public Policy* 29 (2019): 39–94.

[21] Jackson, Vicki C. "Constitutional law in an age of proportionality." *Yale Law Journal* 124 (2014): 3094–3197.

https://doi.org/10.1017/9781009057998.008 Published online by Cambridge University Press

and regulators must be able to navigate these complexities to promote fairness, transparency, and equity. We explore real-world examples, such as predictive systems that identify potential harassers and cases like COMPASS (Cooperation on Migration and Partnerships to Achieve Sustainable Solutions) to gain insight into the ethical and regulatory challenges of trust mechanisms driven by algorithmic data.[22] This discussion provides an apt approach to exploring the country that is most commonly associated with data-driven regulations, particularly in ethical contexts – China.

CHINA'S SOCIAL CREDIT SYSTEM: TRUSTWORTHINESS

The SCS in China provides an important example of how technology can be integrated into regulatory governance. The system combines elements of both automated monitoring and behavioral incentives to promote compliance with legal and social norms.

Initial implementations of the SCS in selected cities integrated traditional financial credit scoring with broader behavioral metrics. The system uses both positive and negative incentives to encourage certain behaviors, offering insights into how technological tools can influence social conduct within specific cultural contexts.[23] This approach reflects a unique cultural context where trust in central government institutions remains relatively high, as evidenced by Kostka's survey findings.[24]

Sheng Zou's study on algorithmic ratings in China argues that the SCS exemplifies the reduction of social issues to numerical metrics, potentially undermining fundamental moral values like trust and trustworthiness.[25] This aligns with our broader discussion on the challenges of fostering genuine voluntary compliance in technologically mediated environments.

What seems to be coming from the studies focusing on SCS is that the widespread adoption of it in China, with four out of five respondents using commercial versions, suggests a cultural predisposition toward accepting technologically driven governance solutions.[26] This acceptance may be rooted in China's collectivist culture and high Power Distance, as discussed in our analysis of Hofstede's cultural dimensions in Chapter 6.

The Chinese case also presents a stark contrast to the Nordic model of trust building that was also discussed in Chapter 6. While both approaches aim to enhance

[22] www.iom.int/compass.

[23] Wong, Karen Li Xan, and Amy Shields Dobson. "We're just data: Exploring China's social credit system in relation to digital platform ratings cultures in Westernised democracies." *Global Media and China* 4.2 (2019): 220–232.

[24] Kostka, Genia. "China's social credit systems and public opinion: Explaining high levels of approval." *New Media & Society* 21.7 (2019): 1565–1593.

[25] Zou, Sheng. "Disenchanting trust: Instrumental reason, algorithmic governance, and China's emerging social credit system." *Media and Communication* 9.2 (2021): 140–149.

[26] See discussion in Kostka. "China's social credit systems and public opinion."

https://doi.org/10.1017/9781009057998.008 Published online by Cambridge University Press

societal cooperation, they employ fundamentally different mechanisms shaped by their respective cultural contexts. Analysis of regulatory approaches in different regions reveals distinct mechanisms for promoting compliance. China's SCS utilizes data-driven monitoring and structured incentive systems, implemented through digital infrastructure. The Nordic regulatory framework, by comparison, builds upon established institutional relationships and community-based compliance norms. These differing approaches reflect how regulatory systems often develop in response to existing social and institutional structures. This variation in regulatory design invites empirical examination of several key questions: What is the end goal, to improve behaviors or also to change intrinsic motivation, social capital, and trust? How do preexisting institutional trust levels affect regulatory outcomes? What role do historical governance patterns play in determining the effectiveness of automated compliance systems? Systematic comparative research across jurisdictions could help identify which elements of technological compliance systems are universally applicable and which require adaptation to local institutional contexts.

BIG DATA AND VOLUNTARY COMPLIANCE

Considering the previous discussion on China's SCS in the already mentioned work with Yotam Kaplan, we examined how big data can be used in ways that are less invasive to individuals' privacy and autonomy.[27] Our research explores the transition from personalization to a situational approach in the context of big data and ethical boundaries. Recent years have seen a remarkable rise in big data's use for predictive decision-making in diverse sectors such as finance, healthcare, and law enforcement.[28] As Julie Cohen notes,[29] big data involves both advanced technology and a process that rapidly analyzes massive data volumes, identifies patterns, and applies data-driven predictions. This results in a wealth of synthesized knowledge.

Big data analytics involves working with immense datasets, often reaching into petabytes, as well as integrating information from various sources.[30] Some of the current applications of big data analytics include spam and fraud detection, credit scoring, insurance pricing, and data-driven law enforcement, such as predicting gun violence and other serious crimes.[31] Using big data for predictive regulation enables regulators

[27] Feldman and Kaplan. "Big data and bounded ethicality," 39.

[28] Christin, Angèle. "From daguerreotypes to algorithms: Machines, expertise, and three forms of objectivity." *ACM Sigcas Computers and Society* 46.1 (2016): 27–32.

[29] Cohen, Julie E. "What privacy is for." *Harvard Law Review* 126.7 (2013): 1904–1933.

[30] For other definitions of big data, see Lazer, David, and Jason Radford. "Data ex machina: Introduction to big data." *Annual Review of Sociology* 43.1 (2017): 19–39 (emphasizing the context dependence of any definition of big data); Mayer-Schönberger, Viktor, and Kenneth Cukier. *Big data: A revolution that will transform how we live, work, and think*. Houghton Mifflin Harcourt, 2013.

[31] Papachristos, Andrew V., David M. Hureau, and Anthony A. Braga. "The corner and the crew: The influence of geography and social networks on gang violence." *American Sociological Review* 78.3

https://doi.org/10.1017/9781009057998.008 Published online by Cambridge University Press

to preemptively engage with potential violators by issuing alerts before any wrongdoing takes place. We argue that this data-driven approach effectively tackles many of the ethical challenges suggested earlier in this chapter. Another important concept that Kaplan and I developed is targeted regulation, which allows regulators to focus on specific risks and behaviors through data-driven law enforcement, rather than random enforcement. This targeted approach is needed to prevent ethical desensitization and enhance ethical deliberation. Additionally, we explore the idea of *tailored regulation*, which involves using data-driven law enforcement to choose appropriate regulatory measures based on insights gained from specific instances of misconduct.

While the focus of my joint work with Kaplan, as discussed, was on the concept of bounded ethicality, the newfound ability to overcome ethical numbing is crucial.[32] To improve ethical deliberation, regulatory intervention must be targeted and specific, rather than broad and general. For example, organizational ethical alerts are effective only if they are targeted and infrequent, rather than routine and constant.[33] If everyone is randomly bombarded with ethical messages, those messages will quickly lose their meaning and impact.[34] Big data analysis can provide a significant advantage here by enabling a regulatory scheme that is activated only when analysis of the background information suggests its involvement is necessary.

TAILORED REGULATION

Using data to inform law enforcement can help overcome the challenge of selecting the most effective methods for promoting thoughtful consideration and addressing ethical limitations. This will be crucial for deciding on the most appropriate legal response, based on the ethical bias that prevents open and honest discussion.

Kaplan and I argue that big data analysis can provide regulators with a wealth of information regarding instances of misconduct, allowing them to develop the most suitable regulatory response. Situations where many of the likely transgressors are first-time offenders tend to involve ethical blind spots, compared to situations where the transgressor is a repeat offender. In these cases, it is less likely that one would be unfamiliar with the underlying ethical problem behind the behavior. In addition, by utilizing big data, we can gain insights into the past transgressions of frequent

(2013): 417–447 (offering a network model that predicts the identity of individuals most likely to participate in gang violence). See also Perry, Walt L. *Predictive policing: The role of crime forecasting in law enforcement operations*. Rand Corporation, 2013.

[32] Ayal, Shahar, et al. "Three principles to REVISE people's unethical behavior." *Perspectives on Psychological Science* 10.6 (2015): 738–741.

[33] See, for example, in environmental context, Ricart, Sandra, Jorge Olcina, and Antonio M. Rico. "Evaluating public attitudes and farmers' beliefs towards climate change adaptation: Awareness, perception, and populism at European level." *Land* 8.1 (2018): 1–24.

[34] Banaji, Mahzarin R., and Anthony G. Greenwald. *Blindspot: Hidden biases of good people*. Bantam, 2016.

https://doi.org/10.1017/9781009057998.008 Published online by Cambridge University Press

offenders and identify the most effective ethical nudges to encourage ethical behavior. Essentially, the history of the violations of the typical transgressor could be used to improve our ability to predict not only the situational characteristics that may lead to more unethical behavior, but also the specific interventions that are likely to be effective based on their past efficacy across different situations.[35]

Further, policymakers may be able to determine indirectly which mechanism is operative by using big data analysis together with an *experimental regulation* approach.[36] Randomized content can be created using experimental design protocols and analyzed for varying effects through big data analysis. By deploying randomized messages, statistical analysis can yield insights into the effectiveness of each message.

INTEGRATED DATASETS

Another aspect that Kaplan and I discuss is the integration of data from previously separate institutional sources.[37] Law enforcement has always been data-driven to an extent. That is, police have traditionally used limited datasets, documenting fingerprints, past convictions, or other relevant information.[38] The trend toward big data involves combining information from multiple sources and analyzing it in a systematic and integrated way.[39] An integrated system like this enables users to track disparate data points in relation to each other and study correlations among data points that originate from different datasets.

In our paper, Kaplan and I demonstrate that the recent trend of using big data for law enforcement purposes marks a departure from traditional approaches. Specifically, there is now a growing move to gather and analyze information about individuals with no prior contact with law enforcement authorities,[40] which is crucial given the recognition that bounded ethicality is far more prevalent, as discussed in the concept of good people in the law.[41]

In that paper, we show how the growing availability of data enables new ways to study patterns of unethical behavior. A great example is Cantalupo and Kidder's

[35] Feldman and Kaplan. "Big data and bounded ethicality," 39.

[36] The more common term is experimental legislation, see Ranchordás, Sofia. "The whys and woes of experimental legislation." *Theory and Practice of Legislation* 1.3 (2013): 415–440, but the term experimental *regulation* is also mentioned frequently and fits under the same analytical framework (415). In both cases, the term refers to the idea that policymakers should aspire to evaluate the effects of legislation or regulation either prior to or after their implementation (417).

[37] Ferguson, Andrew Guthrie. "Big data and predictive reasonable suspicion." *University of Pennsylvania Law Review* 163 (2014): 327–410.

[38] Berk, Richard. "Balancing the costs of forecasting errors in parole decisions." *Albany Law Review* 74 (2010): 1071–1086 (discussing the use of historical data to identify future offenders).

[39] Brayne, Sarah. "Big data surveillance: The case of policing." *American Sociological Review* 82.5 (2017): 977–1008.

[40] Brayne, "Big data surveillance," 992.

[41] Feldman, Yuval. *The law of good people: Challenging states' ability to regulate human behavior*. Cambridge University Press, 2018.

https://doi.org/10.1017/9781009057998.008 Published online by Cambridge University Press

2018 study of faculty sexual harassment in academia. They combined different types of data – news reports, federal investigations, and court cases – to reveal systematic patterns of misconduct. Their approach shows how legal research can now use any collection of documented wrongdoing or disputes as a valuable source for analysis. Contemporary law enforcement entities increasingly possess access to extensive databases – both internally generated and commercially sourced – comprising an exponential magnitude of discrete data points. Through rigorous empirical analysis, these comprehensive datasets enable the identification of contextual variables that correlate with or potentially precipitate unethical conduct. This methodological integration of diverse data repositories represents a significant epistemological advancement in comprehending and addressing multifaceted ethical infractions across varied institutional contexts, thereby offering more sophisticated and efficacious approaches to regulatory compliance and enforcement protocols.

The paper discusses also the work of James Jacobs and Tamara Crepet regarding the fact that private commercial actors may also maintain databases that could prove useful.[42] Financial institutions maintain detailed and extensive records, directly and indirectly documenting the actions, preferences, and behavior of both employees and consumers.[43] Similar datasets are maintained and used by retailers, pharmaceutical companies, and technology firms.[44] Some private companies, especially in the financial sector, have already begun implementing situational regulation of their employees. For example, JPMorgan Chase provides ethical reminders to employees, cautioning them when they are approaching the limits of legitimate business practices. Such warnings, which seek to prevent wrongdoing before it occurs, are based on "predictive-monitoring" algorithms.[45] Other financial institutions are beginning to adopt similar mechanisms based on big data analysis.[46]

THE PERSONALIZED LAW APPROACH

Omri Ben-Shahar and Ariel Porat's influential book on personalized law focuses on the use of technology, particularly big data, as a solution to the fact that people's

[42] Jacobs, James, and Tamara Crepet. "The expanding scope, use, and availability of criminal records." *NYU Journal of Legislation and Public Policy* 11.2 (2008): 177–214.

[43] Jacobs and Crepet. "The expanding scope, use, and availability of criminal records."

[44] Kline, Candice L. "Security theater and database-driven information markets: A case for an omnibus US data privacy statute." *University of Toledo Law Review* 39 (2007): 443–496; Kamin, Sam. "The private is public: The relevance of private actors in defining the Fourth Amendment." *Boston College Law Review* 46 (2004): 83–148 (discussing databases that retailers compile in order to store consumer information).

[45] See, generally, Bennett Moses, Lyria, and Janet Chan. "Algorithmic prediction in policing: Assumptions, evaluation, and accountability." *Policing and Society* 28.7 (2018): 806–822.

[46] Credit Suisse is developing a compliance program with Palantir Technologies, a Silicon Valley tech company focused on data analysis for police and intelligence services; Jeffrey Vogeli, "Credit Suisse, CIA-Funded Palantir to target rogue bankers." *Bloomberg* (March 22, 2016). www.bloomberg.com/news/articles/2016–03–22/credit-suisse-cia-funded-palantir-build-joint-compliance-firm.

https://doi.org/10.1017/9781009057998.008 Published online by Cambridge University Press

preferences differ across many legal domains.[47] In their book, they demonstrate how big data analytics can help the law provide tailored solutions to various factors that predict people's preferences and align them with fairness constraints. Although the book doesn't address people's ethics and willingness to cooperate, it's worth considering how the authors' approach could justify a situation in which past cooperation determines the level of trust the government should have in the public's willingness to cooperate voluntarily.

The concept of personalization could also be incorporated into various technologies, such as modifying the type of a pledge and providing the option to opt-out or omit certain sections. Tax authorities could gain insights into effective practices for promoting ethical behavior among individuals who share similar characteristics. As people increasingly interact with the government through digital platforms, personalization should aim to enhance ethical standards rather than simply learning people's preferences and establishing a legal framework based on that.

EMPATHY IN THE DIGITAL ADMINISTRATIVE STATE

Another important factor in technology's ability to improve voluntary compliance is empathy, which is often absent when algorithms make policy decisions affecting people. In her influential paper, Sofia Ranchordás writes that making mistakes is a fundamental human trait, especially when dealing with complex government forms like tax returns and benefit applications.[48] Nevertheless, the ability to overlook these mistakes is diminishing as government services become more digitized and automated. The author asserts that empathy has been a contentious but vital factor in enabling public officials to strike a balance between administrative priorities and the needs of citizens, particularly underserved groups such as people with disabilities, the elderly, minorities, and those with a low socioeconomic status. In the digital administrative state, the erosion of empathy could potentially hinder vulnerable citizens from being able to access their rights through the digital bureaucracy.

Ranchordás argues that preserving empathy, defined as the capacity to comprehend legal scenarios from various angles and relate to others, is pivotal in the realm of administrative law, especially within the context of the digital administrative state. Empathy can significantly enhance procedural due process, equitable treatment, and the legitimacy of automated systems. Administrative empathy does not promote emotional-based exceptions or individualized justice. Instead, it suggests strategies

[47] Ben-Shahar, Omri, and Ariel Porat. *Personalized law: Different rules for different people*. Oxford University Press, 2021.

[48] Ranchordás, Sofia. "Empathy in the digital administrative state." *Duke Law Journal* 71 (2021): 1341–1390.

https://doi.org/10.1017/9781009057998.008 Published online by Cambridge University Press

to humanize digital governance and automated decision-making by comprehensively understanding citizens' requirements.

Ranchordás explores the significance of empathy in the digital administrative state on two fronts. First, she posits that administrative empathy can address certain deficiencies of digital bureaucracy by acknowledging citizens' diverse competencies and needs, which demands that application forms, governmental platforms, algorithms, and support systems be redesigned. Second, empathy should function as a mean of humanizing administrative decision-making after decisions are taken. Drawing upon comparative instances of empathic practices in the United States, the Netherlands, Estonia, and France, Ranchordás offers an interdisciplinary examination of empathy's role in administrative law and public administration in the digital age, with a focus on empowering vulnerable citizens while also operationalizing the concept of administrative empathy.

REORIENTING BIG DATA LAW ENFORCEMENT

According to researchers, big data has already become incorporated into law enforcement procedures, particularly in the area of algorithmic enforcement.[49] To give one example of this trend, Kaplan and I discuss the case of Palantir Technologies, a privately owned software company specializing in big data analytics.[50] Founded in 2004, Palantir is just one of the major big data platforms currently used by law enforcement agencies in the United States.[51] Palantir customers include the Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), National Security Agency (NSA), United States Department of Homeland Security (DHS), United States Immigration and Costumes Enforcement (ICE), as well as police departments in major American cities such as New York and Los Angeles.[52]

The argument that Kaplan and I presented is that the increased use of data-driven law enforcement has raised significant concerns regarding its legitimacy. Mainly, commentators have voiced objections to this emerging form of law enforcement that relies on big data, citing concerns related to privacy and autonomy concerns.[53]

[49] See Manyika, James. "Big data: The next frontier for innovation, competition, and productivity." *McKinsey Global Institute* 1 (2011): 1–156 (describing police practices in using cellphone information); Ferguson. "Big data and predictive reasonable suspicion," 327–410.

[50] Burns, Matt. "Leaked Palantir doc reveals uses, specific functions and key clients." *TechCrunch* (January 11, 2015). https://techcrunch.com/2015/01/11/leaked-palantir-doc-reveals-uses-specific-functions-and-key-clients/.

[51] Burns. "Leaked Palantir doc reveals uses, specific functions and key clients."

[52] Taipale, Kim A. "Data mining and domestic security: Connecting the dots to make sense of data." *Columbia Science and Technology Law Review* 5 (2003): 1–83 (showing that law enforcement agencies are already utilizing big data analysis in a variety of contexts and arguing it would be unrealistic to expect these practices to stop).

[53] Solove, Daniel J. "Digital dossiers and the dissipation of Fourth Amendment privacy." *Southern California Law Review* 75 (2002): 1083–1168 (highlighting the risk to privacy in a world in which personal data is increasingly held by third parties and not by the individuals who own this data).

https://doi.org/10.1017/9781009057998.008 Published online by Cambridge University Press

They argue that such methods may violate citizens' Fourth Amendment rights.[54] Many studies have shown that big data analysis by policymakers can perpetuate existing discriminatory patterns by replicating them.[55]

In our work, we advocate for a shift in the current practices of big data law enforcement and a reassessment of its objectives and procedures. We demonstrate that prioritizing the ordinary unethicality of normative people, as the primary objective of big data law enforcement, can alleviate some of the valid concerns about law enforcement use of big data analytics.

There are two main reasons why this is true. First, governments don't need to collect information at the personal level in order to overcome bounded ethicality. Unlike the use of big data in other contexts, such as preventing serious crimes, the purpose of government intervention is not to target particularly malevolent individuals but to identify the conditions that lead to ethical biases among ordinary people. This suggests that privacy concerns are relatively less alarming in this context because information does not necessarily have to be linked to particular individuals. Likewise, concerns about the perpetuation of prejudice and discriminatory actions are less concerning, since big data analysis is used to produce situational forecasts instead of personalized ones.

ALGORITHMIC REGULATION

As regulators discuss the potential of algorithms to help with trust issues, it is important to recognize that there has already been an increase of research on algorithmic regulation.[56] In her influential analysis of algorithmic regulation, Karen Yeung examines how automated decision-making systems manage risk and shape behavior through continuous data collection and computational analysis. She develops a comprehensive taxonomy, distinguishing between reactive and preemptive systems, while identifying eight distinct regulatory forms based on three key operational stages: standard setting, information gathering and monitoring, and enforcement through sanctions and behavioral modification.

Drawing on interdisciplinary perspectives, Yeung evaluates critical questions about the legitimacy of algorithmic governance. Her framework is particularly valuable for understanding how automated systems can function both as standalone regulatory tools and as supplements to traditional enforcement mechanisms.

[54] Ferguson, Andrew Guthrie, "Big data and predictive reasonable suspicion." *University of Pennsylvania Law Review* 163 (2014): 327–410 (evaluating the constitutionality of the use of big data analytics as a basis for police searches and seizures).

[55] Barocas, Solon, and Andrew D. Selbst. "Big data's disparate impact." *California Law Review* 104 (2016): 671–732 (on the importance of the data for which the algorithms are being paid).

[56] Yeung, Karen. "Algorithmic regulation: A critical interrogation." *Regulation & Governance* 12.4 (2018): 505–523.

https://doi.org/10.1017/9781009057998.008 Published online by Cambridge University Press

This analysis provides crucial insights into the growing complexity of technology-enabled compliance systems.

ALGORITHMIC POLICING

Furthermore, in examining algorithmic regulation, we must consider how automated enforcement affects compliance and trust. While technology offers the promise of more efficient and consistent enforcement, research indicates it may actually erode public trust and create new challenges for voluntary compliance – dynamics we'll examine in detail in the next section.

These concerns are particularly evident in law enforcement, where new technologies can amplify existing social inequities.[57] Consider predictive policing algorithms, which analyze crime data to anticipate likely crime locations and guide police deployment.[58] While seemingly objective, these systems learn from historical data that reflects long-standing racial biases in policing practices, thereby risking the perpetuation and automation of discriminatory patterns. The equity challenge extends to facial recognition technologies used by police departments – these systems have shown significantly lower accuracy rates when identifying people of color, increasing the risk of wrongful identification and prosecution.[59] Recognizing these systemic risks, researchers are now developing comprehensive frameworks to evaluate the equity impact of police technologies before deployment.[60]

In another survey, the participants expressed doubts about an algorithm's ability to identify good candidates, reasoning that it would lack human intuition and make judgments based on keywords or ignore qualities that are hard to quantify. These results indicate that people have a lower level of trust in algorithms performing such tasks.[61] Other studies have examined police responses to new technology, focusing on the benefits of data integration as well as on the number of risks associated with different pathways. These algorithmic biases can disproportionately harm vulnerable populations, magnifying existing social and economic disadvantages.[62]

[57] Bennett Moses and Chan. "Algorithmic prediction in policing."

[58] Benbouzid, Bilel. "To predict and to manage: Predictive policing in the United States." *Big Data & Society* 6.1 (2019): 1–13.

[59] Kevorkian, Martin. *Color monitors: The black face of technology in America*. Cornell University Press, 2018.

[60] Moy, Laura M. "A taxonomy of police technology's racial inequity problems." *University of Illinois Law Review* (2021): 139–192.

[61] Lee, Min Kyung. "Understanding perception of algorithmic decisions: Fairness, trust, and emotion in response to algorithmic management." *Big Data & Society* 5.1 (2018):1–16.

[62] Chan, Janet, and Lyria Bennett Moses. "Making sense of big data for security." *British Journal of Criminology* 57.2 (2017): 299–319.

https://doi.org/10.1017/9781009057998.008 Published online by Cambridge University Press

TECHNOLOGICAL SURVEILLANCE AND TRUST

Governments use technological surveillance as a substitute for trusting people.[63] This shift is particularly evident in the evolution from traditional panoptic surveillance to newer forms of environmental monitoring, as exemplified by predictive policing. Predictive policing aims to forecast where and when future crimes will occur. However, finding the appropriate balance between predictive accuracy and protecting historically disadvantaged groups is a challenging and subjective task. Moreover, research has highlighted concerns about law enforcement officers' compliance with necessary safeguards.[64] Given the public's distrust of these systems, independent judicial oversight may be necessary. As a model for building public confidence, governments could apply the same rigorous controls to these new surveillance systems that they use for handling online tax returns.[65]

The New York City Police Department has transitioned from traditional policing methods to those based on predictive analytics in response to a growing demand for police services. This has resulted in regularly suspecting certain groups of people based on their perceived risks and threats.[66] In addition to the problematic nature of predicting analytics, there is also the problem of transparency in these algorithms, which is sometimes lacking in AI-driven policing.[67]

TRANSPARENCY AND TRUST

Research has shown that higher levels of citizen satisfaction with the level of interaction with government are associated with higher levels of trust in government. Similarly, the more citizens believe that government websites are reliable sources of information, the greater their level of trust in government.[68]

The increasing adoption of e-government strategies has significant implications for public administration and citizen engagement. Research suggests that the use of government websites may lead to positive attitudes toward e-government, which

[63] Trüdinger, Eva-Maria, and Leonie C. Steckermeier. "Trusting and controlling? Political trust, information and acceptance of surveillance policies: The case of Germany." *Government Information Quarterly* 34.3 (2017): 421–433.

[64] Ferguson, "Big data and predictive reasonable suspicion," 327.

[65] Warkentin, Merrill, et al. "Encouraging citizen adoption of e-government by building trust." *Electronic Markets* 12.3 (2002): 157–162.

[66] Sanders, Carrie B., and James Sheptycki. "Policing, crime and 'big data': Towards a critique of the moral economy of stochastic governance." *Crime, Law and Social Change* 68.1 (2017): 1–15.

[67] E.g., Berk, Richard A. "Artificial intelligence, predictive policing, and risk assessment for law enforcement." *Annual Review of Criminology* 4 (2021): 209–237.

[68] Welch, Eric W., and Charles C. Hinnant. "Internet use, transparency, and interactivity effects on trust in government." In *Proceedings of the 36th Annual Hawaii International Conference on System Sciences*, edited by Ralph H. Sprague Jr, IEEE, 2003: 144a.1–144a.7.

https://doi.org/10.1017/9781009057998.008 Published online by Cambridge University Press

in turn can foster improved trust and confidence in governments generally.[69] This digital transformation has the potential to enhance the provision of many types of public services, making them more accessible and efficient.

A study by Tolbert and Mossberger (2006)[70] supports this view, arguing that the growing number of government websites at the federal level correlates with a rise in the perception of government transparency. This increased perception of transparency is crucial, as it can lead to greater citizen participation and a more informed electorate.

However, as governments increasingly rely on digital tools and data analytics to inform decision-making and service delivery, new challenges emerge. For instance, many analysis tools used in public administration tend to focus on specific locations rather than on individual citizens.[71] While this approach can be useful for urban planning and resource allocation, it may overlook the nuanced needs of diverse populations.

Furthermore, it is crucial to acknowledge that achieving complete neutrality in data-driven governance may be impossible, particularly when dealing with historical data. Such data often includes evidence of past discrimination, which can inadvertently perpetuate biases if not carefully addressed. This challenge highlights the need for critical examination of the data and algorithms used in e-government initiatives.[72]

The ability to predict the geographic distribution of future crimes, regardless of accuracy, alters the context in which police strategies are developed. Some predictive programs focus on mobilizing police patrols to specific blocks using predictive analytics instead of trying to comprehend the underlying causes of crime in a particular area.[73] While police resistance may hinder the implementation of predictive policing, empirical evidence demonstrates that hot spot policing effectively reduces crime levels.[74] Hot spots should be limited in size, so they can be patrolled effectively, and there should not be too many of them.

In the context of taxes, numerous research findings suggest that enforcing regulations too strictly, with high audit rates and heavy fines, may result in reactance and resistance-provoking compliance.[75] Research shows that the successful

[69] Tan, Chee Wee, Izak Benbasat, and Ronald T. Cenfetelli. "Building citizen trust towards e-government services: Do high quality websites matter?" In *Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008)*, edited by Ralph H. Sprague Jr, IEEE, 2008: 217–217.

[70] Tolbert, Caroline J., and Karen Mossberger. "The effects of e-government on trust and confidence in government." *Public Administration Review* 66.3 (2006): 354–369.

[71] West, Darrell M. "E-government and the transformation of service delivery and citizen attitudes." *Public Administration Review* 64.1 (2004): 15–27.

[72] Bennett Moses and Chan. "Algorithmic prediction in policing."

[73] Brayne, Sarah. *Predict and surveil: Data, discretion, and the future of policing*. Oxford University Press, 2020.

[74] Brayne, Sarah. *Predict and surveil*.

[75] Murphy, Kristina. "Enforcing tax compliance: to punish or persuade?" *Economic Analysis and Policy* 38.1 (2008): 113–135.

https://doi.org/10.1017/9781009057998.008 Published online by Cambridge University Press

implementation of e-audits depends on acceptance by both taxpayers and tax auditors.[76] Precise and accurate tax audits can significantly increase public trust in tax authorities without making the authorities appear more coercive. As discussed in previous chapters, trust promotes voluntary compliance, while enforcement capacity ensures compliance through deterrence. Nevertheless, tax authorities must maintain sufficient enforcement capabilities to ensure overall compliance.[77]

Taxpayers who already have a high level of trust in tax authorities are more likely to support e-audits and respond to them by increasing their trust even further.[78] There is a positive association between electronic participation and people's perceptions of government responsiveness and their trust in the local government providing the program.[79] E-participants who receive quality feedback and responses from government officials are more likely to perceive that they have obtained useful policy information that helps them better understand government agencies and community issues. The quality of government responses to citizen participants can help boost e-participants' self-esteem.[80]

By improving the frequency and quality of its communication with citizens, the government can strengthen its relationship with the people and demonstrate that its actions are in their best interest. This sense of connection with the government could also contribute to increased trust among citizens.

There is a significant gap in research on the factors that build trust and lead to the successful adoption of e-government services. While studies have shown that trust in e-government is influenced by various factors – including gender, education, perceived risk, and citizens' expectations and beliefs – very few have examined how trust affects satisfaction, continued usage, and successful e-government adoption.[81] The accuracy, completeness, reliability, and accessibility of information on government websites are crucial factors that influence citizens' trust. In addition, timely updates to the system can also influence the level of trust citizens have in the information provided.

Further research on the correlation between trust and technology indicates that citizens' trust in the government rises when they receive information about

[76] De Santis, Federica, and Giuseppe D'Onza. "Big data and data analytics in auditing: In search of legitimacy." *Meditari Accountancy Research* 29.5 (2021): 1088–1112.

[77] Brezina, Paul, Eva Eberhartinger, and Maximilian Zieser. *The future of tax audits? The acceptance of online-based, automated tax audits and their effects on trust and power*. WU Vienna University of Economics and Business, 2021.

[78] Brezina, Eberhartinger, and Zieser. The future of tax audits?

[79] Kim, Soonhee, and Jooho Lee. "E-participation, transparency, and trust in local government." *Public Administration Review* 72.6 (2012): 819–828.

[80] Kim and Lee. "E-participation, transparency, and trust in local government."

[81] Alzahrani, Latifa, Wafi Al-Karaghouli, and Vishanth Weerakkody. "Analysing the critical factors influencing trust in e-government adoption from citizens' perspective: A systematic review and a conceptual framework." *International Business Review* 26.1 (2017): 164–175.

https://doi.org/10.1017/9781009057998.008 Published online by Cambridge University Press

government actions and processes. Having the users participate in the process, as well as consulting them for their views, is an imperative approach to creating trust.[82]

If government agencies expect citizens to provide sensitive information and carry out personal transactions online, they must recognize and enhance citizens' views concerning the reliability of e-government services.[83] Government agencies must acquire and advertise features that increase citizens' perceptions of the site's trustworthiness as well.[84]

SUMMARY

This chapter looks at how technology affects people's willingness to follow rules without being forced. We pay special attention to two main tools: systems that track reputation and subtle prompts that encourage certain behaviors. While technology can help promote compliance without heavy-handed enforcement, it creates an interesting dilemma. Better technological monitoring might mean we need to rely less on trust, but it could also weaken people's natural motivation to cooperate voluntarily.[85]

We examined the promise and perils of big data and algorithmic regulation in identifying trustworthy individuals and tailoring regulatory approaches. We then addressed the ethical concerns surrounding data-driven trust mechanisms, including privacy issues and potential reinforcement of biases.[86] The importance of transparency and empathy in digital governance to maintain public trust is emphasized, along with the challenges of balancing technological efficiency with human discretion and empathy in administrative processes.[87]

In this chapter, we explore how new technologies fit into our overall understanding of voluntary compliance. While technology gives us new ways to encourage rule following, we need to be thoughtful about how we use these tools. As we've seen throughout the book, getting people to willingly follow rules depends on their inner motivation and trust in the system. Technology could either help build these qualities or wear them down, depending on how it's used.

FUTURE RESEARCH DIRECTIONS

Future research should focus on empirical studies examining technological personalization and the long-term effects of technological nudges and reputation systems

[82] Alzahrani, Al-Karaghouli, and Weerakkody. "Analysing the critical factors influencing trust in e-government adoption from citizens' perspective."
[83] Bélanger, France, and Lemuria Carter. "Trust and risk in e-government adoption." *Journal of Strategic Information Systems* 17.2 (2008): 165–176.
[84] Bélanger and Carter. "Trust and risk in e-government adoption."
[85] Yeung. "Algorithmic regulation."
[86] Barocas and Selbst. "Big data's disparate impact," 671.
[87] Ranchordás. "Empathy in the digital administrative state," 1341.

https://doi.org/10.1017/9781009057998.008 Published online by Cambridge University Press

on enhancing intrinsic motivation and voluntary compliance. Comparative analyses of different technological approaches to compliance across various cultural contexts would build on the insights from Chapter 6, providing a more comprehensive understanding of how cultural factors interact with technological interventions.[88]

Investigations into the optimal balance between algorithmic decision-making and human discretion in regulatory processes are crucial, as are explorations of how emerging technologies such as blockchain and AI might reshape voluntary compliance paradigms.[89] Studies on the psychological impact of continuous technological monitoring on individuals' sense of autonomy and trust in institutions would provide valuable insights into the potential unintended consequences of these approaches.

Research should also focus on designing technology-enhanced regulatory systems that preserve or enhance intrinsic motivation and on developing ethical frameworks for the use of big data in predictive compliance models, with a focus on fairness and privacy preservation. Examination of how different demographic groups across different regulatory contexts respond to technologically mediated compliance strategies would help ensure that these approaches are inclusive and effective across diverse populations.[90]

Future research should examine whether technology can help create regulatory approaches that match different people's values and preferences. We also need to better understand how people's comfort with technology affects their acceptance of digital compliance systems. These insights would help clarify the benefits and limitations of using technology to encourage voluntary compliance in today's increasingly digital environment.

[88] Luria, Gil, Ram A. Cnaan, and Amnon Boehm. "National culture and prosocial behaviors: Results from 66 countries." *Nonprofit and Voluntary Sector Quarterly* 44.5 (2015): 1041–1065.

[89] Hawlitschek, Notheisen, and Teubner. "The limits of trust-free systems."

[90] Ferguson, Andrew Guthrie. "Whom we police: person-based predictive targeting." In *The rise of big data policing: Surveillance, race, and the future of law enforcement*. New York University Press, 2017: 34–61.

https://doi.org/10.1017/9781009057998.008 Published online by Cambridge University Press