## **Chapter 7. Technology, Nudges, Reputation, and Voluntary Compliance[[1]](#footnote-1)**

Contents

**[Chapter 7. Technology, Nudges, Reputation and Voluntary Compliance:](#_Toc168483574)** [1](#_Toc168483574)

[Introduction 1](#_Toc168483575)

[The Monitoring Everything Challenge 2](#_Toc168483576)

[Technology as a Way to Enhance Communication Between People and Government 3](#_Toc168483577)

[Technology – More Monitoring, Less Trust? 3](#_Toc168483578)

[Cameras in Public Spaces and Trust 4](#_Toc168483579)

[Regulating Situations vs. Regulating People 4](#_Toc168483580)

[Proportionality and Behavioral Big data 5](#_Toc168483581)

[China’s Social Credit System – Trustworthiness 6](#_Toc168483582)

[Big Data and Voluntary Compliance 7](#_Toc168483583)

[Tailored Regulation 8](#_Toc168483584)

[Integrated Datasets 8](#_Toc168483585)

[The Personalized Law Approach 10](#_Toc168483586)

##

## Introduction

This chapter explores whether technology can be used to enhance non-coercive 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. The second question is whether technology can help identify which parts of the population can be trusted to comply voluntarily. It is important to note that, on the surface, the second goal may appear to resemble the Chinese social credit system that seeks to exploit technology in order to enable the state to monitor and control people’s social behavior. 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 towards more people.

Generally speaking, using technology to enhance compliance could lead to two developments. On the one hand, it is possible that using improved technology monitoring could lead to a reduced need to rely on the goodwill of people to comply voluntarily. By providing clear instructions and analyzing how people will behave, it may be possible to complement research on personalization[[2]](#footnote-2) and technology-based enforcement,[[3]](#footnote-3) as well as reduce some of the need for reliance on people’s goodwill. 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.

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.[[4]](#footnote-4)

Research conducted in the field of algorithmic management has produced mixed results regarding the potential crowding-out effect of rating and monitoring procedures. 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. Therefore, in this chapter, we will examine the potential pitfalls of using technology as a substitute for state enforcement.

## The Monitoring Everything Challenge

As noted above, the primary challenge in using technology is determining whether we can achieve a level of monitoring that renders the need to trust people unnecessary by enabling us to monitor nearly every action 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 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 is the case in several aspects. Firstly, people are not being monitored all the time. Furthermore, 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. Therefore, the state found it easier to monitor areas where voluntary compliance posed less of a problem, as it was epidemiologically less risky. It was much more difficult for the state to enforce COVID regulations in closed spaces where more of the virus transfer could happen.[[5]](#footnote-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 those people who were 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 focus on a few elements of the interaction between technology and voluntary compliance:

1. Technology has an impact on the relationship between people and the government, and can sometimes limit the flexibility of human decision-making. In situations where technology is not being utilized, cutting corners may be more common.
2. Technological advancements have improved enforcement, making it necessary for governments to rely on people’s voluntary compliance, This provision also enables the government to distinguish between individuals based on their previous actions, which is also pertinent to the following point.
3. Technology is enhancing the level of personalization in regulation, enabling a more individualized and differentiated approach to regulation. This, in turn, makes it easier for people to feel that the regulation is consistent with their personal preferences.
4. Technological advancements have led to an increased ability to design incentives, creating opportunities for incentivized voluntary compliance. This could eventually lead to voluntary compliance being internalized over the long term.

## Technology as a Way to Enhance Communication Between People and Government

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. 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.[[6]](#footnote-7) 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.[[7]](#footnote-8) 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.

## Technology – More Monitoring, Less Trust?

In many ways, the role of law and technology revolves around questions of trust and people’s ability to trust technology On one hand, as mentioned in the introduction, 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. A classic example of how technology improves monitoring is through the use of 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 take into account newer advancements such as Bitcoin, which are even more challenging to monitor by authorities.

For 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. Similarly, renting through booking websites like Airbnb is less likely to be vulnerable to tax evasion.[[8]](#footnote-9) Furthermore, services like Airbnb, Uber, and Lyft not only help to reduce tax evasion but also offer ways for the public to determine who they can trust based on reputation and reporting systems.[[9]](#footnote-10)

## Cameras in Public Spaces and Trust

The goal of technology is to simplify the process for states to 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? The anti-cash revolution may change the need for trust in taxation. Has it been successful so far? Do we prefer nudges to contact tracing apps or epidemiological interviews with people who got infected?[[10]](#footnote-11)

## Regulating Situations vs. Regulating People

The new paper by Chapter and Lowenstein[[11]](#footnote-12) and other research possibly support the view that technological advancements may reduce the need to change intrinsic motivation. When discussing corporate responsibility for climate change, they suggest that we should prioritize the development of technology that can help reduce the burden placed on individuals to address this issue.

This book’s attempt to identify intrinsic motivation among people is limited in scope considering the complexity of the subject. Technology has the potential to replace individual responsibility and behavioral change.

Put another way, do technologies serve as a substitute for an innate transformation? Or do they augment it by allowing states to shift their focus away from whom to trust in favor of advancing to the next level by prioritizing factors such as compliance quality, which was discussed in the first chapter.

## Proportionality and Behavioral Big data

In collaboration with Ori Aronson and Orly Lobel,[[12]](#footnote-13) we are examining the constitutionality of differentiating between people based on their past behavior and building data-based trust in groups and individuals. The computational powers of algorithms present an opportunity to move beyond concealing information due to privacy and equality concerns and instead pursue a new paradigm of fairness through awareness. AI’s ability to identify patterns based on proxies for identity holds immense potential but also presents significant risks. Our paper examines the ethical and regulatory hurdles of algorithmic data-driven trust methods that improve trust in individuals for regulatory purposes. These methods have relevance in various regulatory contexts as they involve assessing trustworthiness at both individual and group levels. By utilizing machine learning, data can be aggregated to create individual profiles, which can pose questions about their societal acceptance, as mentioned in relation to “compliance scores.” Moreover, it raises concerns regarding norm violations that may affect an individual’s overall trustworthiness score, which includes elements such as accuracy, legality, and morality. Trust at the group level depends on data linking compliance to group affiliations, but this can lead to reinforcing biases and class disparities, particularly for marginalized communities.

In our collaborative work,[[13]](#footnote-14) we aim to fill the gap in current research on big data by exploring the feasibility and desirability of utilizing big data for regulatory decision-making. In the context of trust-based regulation, we focus on the challenge of identifying trustworthy individuals within the public. Specifically, we delve into the ability to anticipate and evaluate public cooperation, particularly during the early stages of the COVID-19 pandemic. At that time, governments had to determine whether they could depend on public confidence to adhere to safety protocols. Big data has the potential to accurately distinguish individuals and groups, which can enable more precise predictions of voluntary cooperation in trust-based regulation. These questions are important for less coercive regulatory systems. Trust works in a reciprocal manner, meaning that placing trust in individuals can enhance their trustworthiness. While the idea of suspecting individuals might intuitively lead to changes in behavior, there is less empirical research on this issue.

The Fourth Amendment safeguards individuals from unreasonable police searches and seizures. Utilizing big data will have an impact on all the main facets of traditional policing, including the practice of stop and frisk. The more information that is known or discovered about a suspect, the easier it is to justify a stop based on reasonable suspicion. However, relying on big data to make these decisions can lead to mistakes as well as violations of the right to privacy. Big data can also overwhelm officers and interfere with their ability to determine who should be stopped for suspected criminal activity.[[14]](#footnote-15)

We delve deeper into ethical considerations surrounding the regulation of trust in data-driven settings. Specifically, we examine the ethical implications of differentiated approaches to lawmaking and regulation, with a particular emphasis on regulating trust based on data. In this context, we are outlining key ethical considerations. For example, we ask what is the meaning of statistical trust. What degrees of effect are required to justify a policy change? What levels of correlation can be considered predictive enough to warrant different treatments? What policy purposes justify predictions, and security concerns, or provide more efficient ways to collect taxes? According to the proportionality doctrine in constitutional law, policymakers may engage in activities that have a higher likelihood of infringing on people’s rights if the goal they are attempting to achieve is of greater importance.

Overall, the collaboration 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 and regulators must be able to navigate these complexities in order to promote fairness, transparency, and equity. In our collaborative work, we explore real-world examples, such as predictive systems that identify potential harassers and cases like COMPASS to gain insight into the ethical and regulatory challenges of trust mechanisms driven by algorithmic data.

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 Social Credit System (SCS) in China has generated concerns globally about the possibility of an Orwellian dystopia powered by technology. A study s conducted on the use of algorithmic ratings in everyday life in China[[15]](#footnote-16) argues that the SCS is an exemplar of how social issues are often reduced to numbers and statistics. This approach undermines important moral values, such as trust and trustworthiness.[[16]](#footnote-17) Current research indicates that China is conducting a pilot of its expansive SCS in select cities,[[17]](#footnote-18) aiming to merge financial credit scores with broader societal assessments. The SCS employs a system of rewards and punishments to encourage adherence to government values and discourage – and penalize – deviations. The SCS tackles trust and integrity issues in Chinese society within the world’s largest surveillance network, comprising 176 million cameras (projected to reach 626 million by 2020) used for identity verification and access control. According to existing research, China’s rapid adoption of big data in governance has led to widespread approval of SCSs. According to an online survey conducted in China, four out of five respondents use commercial SCS while only 7% knew about locally run government systems.[[18]](#footnote-19)

Based on the survey, the majority (59%) of individuals believe that the central government should be responsible for managing a nationwide social media surveillance system. Trust in political institutions varies, with a preference for the central government over local ones. In summary, Chinese citizens apparently perceive the SCS as a means to improve their quality of life and bridge institutional gaps in a data-driven governance landscape.

Additional research conducted in China analyzed how algorithmic rating has infiltrated daily life, applying the Frankfurt School’s critique of instrumental reason.[[19]](#footnote-20) Sheng Zou's research provides an excellent example of how to tackle the issue of technological monitoring comprehensively. It demonstrates how the method used by algorithmic systems to gauge trust reflects the growing impact of technology and instrumental reasoning on society. This approach prioritizes identifying patterns and correlations in data over traditional scientific verification methods. As a result, the emphasis shifts from building human relationships to prioritizing technical efficiency, which can reduce trust to mere confidence in technology. This, in turn, can discourage people from taking risks. The SCS in China, which combines economic and social behavior, is a prime example of this growing trend of technologized governance. However, Zou argues that cultivating genuine trust demands a different approach that goes beyond mere instrumentality and avoids an excessive emphasis on quantification.

## Big Data and Voluntary Compliance

In light of the previous discussion on China’s SCS, Yotam Kaplan and I have collaborated on a new project to explore how big data can be used in ways that are less invasive to individuals' privacy and autonomy. 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.[[20]](#footnote-21) As Julie Cohen notes,[[21]](#footnote-22) big data involves both advanced technology and a process that rapidly processes 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.[[22]](#footnote-23) 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[[23]](#footnote-24) and serious crimes.[[24]](#footnote-25)

Using big data for predictive regulation enables regulators to preemptively engage with potential violators by issuing alerts before any wrongdoing takes place. This data-driven approach effectively tackles ethical challenges. Another important concept that we develop is targeted regulation, which allows regulators to focus on specific risks and behaviors through data-driven law enforcement, rather than random enforcement. A 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. Big data analysis can aid in predicting the effectiveness of ethical interventions by taking into account the past histories and situational characteristics of transgressors.

While the focus of the work with Kaplan, as discussed above, was on the concept of bounded ethicality, the newfound ability to overcome ethical numbing is crucial.[[25]](#footnote-26) To improve ethical deliberation, regulatory intervention must be targeted and specific, rather than broad and general. For example, ethical alerts are effective only if they are targeted and infrequent, rather than routine and constant.[[26]](#footnote-27) If everyone is randomly bombarded with ethical messages, those messages will quickly lose their meaning and impact.[[27]](#footnote-28) 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.

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 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.[[28]](#footnote-29)

Second, policymakers may be able to determine indirectly which mechanism is operative by using big data analysis together with an approach of *experimental regulation*.[[29]](#footnote-30) 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.[[30]](#footnote-31) Law enforcement has always been data-driven to an extent. That is, police have traditionally used limited data sets, documenting fingerprints, past convictions, or other relevant information.[[31]](#footnote-32) The trend towards big data involves combining information from multiple sources and analyzing it in a systematic and integrated way.[[32]](#footnote-33) 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.[[33]](#footnote-34) Policymakers are now able to regulate people with no prior encounters with the law, which is crucial given the recognition that bounded ethicality is far more prevalent, as discussed in the concept of good people in the law.[[34]](#footnote-35)

Such an integrated approach can be seen in the recent work of Nancy Cantalupo and William Kidder, who utilized the latest advances in data availability to analyze and categorize instances of sexual harassment by university faculty members.[[35]](#footnote-36) They use a database drawn from media reports,[[36]](#footnote-37) federal civil rights investigations by the United States Departments of Education and Justice,[[37]](#footnote-38) lawsuits by students alleging sexual harassment,[[38]](#footnote-39) and lawsuits by tenure-track faculty fired for sexual harassment.[[39]](#footnote-40) In general, many types of databases are currently accessible for integrated, data-driven law enforcement. Any dataset that documents or records misconduct or disputes can become a relevant source of information.[[40]](#footnote-41)

First, databases currently utilized and upheld by law enforcement agencies can be useful in detecting patterns of unethical conduct. Law enforcement datasets have become increasingly comprehensive over time, providing rich and detailed information that includes data points measured in the trillions. This has happened even before the integration of datasets. These sources include datasets compiled by law enforcement agencies themselves, as well as databases compiled by private companies for use by law enforcement agencies. When analyzed correctly, the data currently available can be essential for identifying and characterizing the specific details of situations that encourage unethical behavior.

According to James Jacobs and Tamara Crepet,[[41]](#footnote-42) private commercial actors may also maintain databases that could prove useful. Financial institutions maintain detailed and extensive records, directly and indirectly documenting the actions, preferences, and behavior of both employees and consumers.[[42]](#footnote-43) Similar datasets are maintained and used by retailers, pharmaceutical companies, and technology firms.[[43]](#footnote-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.[[44]](#footnote-45) Other financial institutions are beginning to adopt similar mechanisms based on big data analysis.[[45]](#footnote-46)

## The Personalized Law Approach

Omri Ben-Shachar and Ariel Porat’s influential book on personalized law[[46]](#footnote-47) focuses on the use of technology, particularly big data, as a solution to the fact that peoples’ preferences differ across many legal domains. 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 their approach could justify a situation in which past cooperation determines the level of trust the government should have in their 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 their preferences and establishing a legal framework based on that.

Empathy in the Digital Administrative State[[47]](#footnote-48)

Another important factor in technology’s ability to improve voluntary compliance is empathy, which is often absent when algorithms make policy decisions affecting people. Sofia Ranchordas writes that making mistakes is a fundamental human trait, especially when dealing with complex government forms like tax returns and benefit applications. 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, elderly persons, minorities, and those with low incomes. 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. Ranchordas 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 to humanize digital governance and automated decision-making by comprehensively understanding citizens' requirements.

Ranchordas 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. Secondly, empathy should function as a means 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, Ranchordas 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.

Top of Form

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.[[48]](#footnote-49) To give one example of this trend, consider the case of Palantir Technologies, a privately owned software company specializing in big data analytics.[[49]](#footnote-50) Founded in 2004, Palantir is just one of the major big data platforms currently used by law enforcement agencies in the United States.[[50]](#footnote-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.[[51]](#footnote-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.[[52]](#footnote-53) They argue that such methods may violate citizens’ Fourth Amendment rights.[[53]](#footnote-54) Many studies have shown that big data analysis by policymakers can perpetuate existing discriminatory patterns by replicating them.[[54]](#footnote-55) In this chapter, 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 bounded ethicality as the primary objective of big data law enforcement can alleviate some of the valid concerns about law enforcement’s 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 in research on algorithmic regulation.[[55]](#footnote-56) Karen Yeung’s study focuses on algorithmic regulation, which is a decision-making process that manages risks and alters behaviors by continuously collecting data and performing computational analysis. The research categorizes these systems as either reactive or preemptive and outlines eight different forms based on their configuration at three stages: standard setting, information gathering and monitoring, and sanctioning and behavioral modification. This study examines the emerging debates on algorithmic regulation, drawing insights from different disciplines to underscore concerns about its legitimacy. Yeung’s descriptive analysis enhances our understanding of the complex nature and potential implications of algorithmic regulation, also in the context of compliance, with and without additional enforcement measures.

Algorithmic Policing

Furthermore, to complement the previous discussion on algorithmic regulation, it is important to consider algorithmic enforcement. In this context, a key question is whether the prevailing research perspective views it as a tool that is unlikely to crowd out willingness to comply with rules. Generally, most studies suggest that technology might reduce rather than increase public trust, as will be outlined in the next section.

For example, concerns have been raised that new police technologies may aggravate existing inequities in policing.[[56]](#footnote-57) For instance, law enforcement agencies in many cities utilize predictive policing algorithms to analyze data on criminal activity and utilize the resulting patterns to anticipate where crimes are more probable to happen. They then deploy police personnel proactively to these locations. However, because the underlying data encodes existing racial inequity in policing, predictive policing may learn and replicate racial bias. A second example is the use of automated face recognition technology by many police forces to identify suspects captured in photos and videos of crimes. Due to the fact that face recognition technology often works less well on faces of color, police face recognition technology may increase the likelihood that people of color will be wrongfully identified and prosecuted for crimes they did not commit. Therefore, current research aims to mitigate such fears by offering various models for assessing the equity impact assessment of proposed police technologies.[[57]](#footnote-58)

In another survey, the participants expressed doubt 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.[[58]](#footnote-59) 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 risks can affect the likelihood and degree of impact on those who could be considered the potential “losers.”[[59]](#footnote-60)

Governments use technological surveillance as a substitute for trusting people. Surveillance is also a mode of engagement with the world that enhances trust, accountability, and eventually responsible humanitarianism. The difference between panoptic modes of surveillance and emerging practices of environmental surveillance can be examined using predictive policing as an example.[[60]](#footnote-61) Predictive policing involves the concept of being able to predict where and when the next crime or series of crimes will occur. Finding the appropriate balance between ensuring predictive accuracy and protecting historically disadvantaged groups is a challenging and subjective task. Previous research has raised concerns about the potential failure of law enforcement officers to comply with necessary safeguards.[[61]](#footnote-62) Due to public distrust, it may be necessary to employ an independent judicial body for assistance. Governments can reassure citizens that the same rigorous controls applied to government handling of traditional tax returns also apply to online tax returns.[[62]](#footnote-63)

The survey queried citizens about their experience, involvement, and perceptions of e-government.[[63]](#footnote-64) Among other findings, it revealed people may view such communication approaches as primarily beneficial to the government.

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.[[64]](#footnote-65)

Related to the issue of the lack of trust in big data-based policing is the problem of transparency, which is sometimes lacking in AI-driven policing.[[65]](#footnote-66)

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 that citizens believe that government websites are a reliable source of information, the greater their level of trust in government.[[66]](#footnote-67)

Use of government websites may lead to positive attitudes toward e-government, which may encourage improved trust or confidence in government generally. In other words**,** e-government has the potential to enhance the provision of many types of public services. We maintain that the growing number of government websites at the federal level are connected to a rise in the perception of the transparency of government.[[67]](#footnote-68) Most prediction software tends to focus on locations rather than on people. However, it is crucial to acknowledge that complete neutrality may be impossible to achieve when dealing with historical data, which often includes evidence of past discrimination.[[68]](#footnote-69)

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. Resistance from the police may pose a hindrance to the effective implementation of predictive policing. In addition, t 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.Research indicates that in order for e-audits to be successfully implemented, both taxpayers and tax auditors most widely accept them. Having a high degree of certainty in tax audits can greatly enhance people’s trust in the tax authorities but with no significant effect on how powerful they are perceived to be. We suggest that suggests that trust leads to voluntary compliance and power can ensure enforced compliance. However, we acknowledge that tax authorities must possess a reasonable amount of power in order to ensure compliance.[[69]](#footnote-72)

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. Tax auditors react negatively to the same feature of auditing that makes it attractive to taxpayers, namely audit certainty.[[70]](#footnote-73) 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.[[71]](#footnote-74) 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 their self-esteem.[[72]](#footnote-75) In that regard, a recent study found that citizens are more likely to return to the e-government site if they believe it is more transparent.[[73]](#footnote-76)

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 taken in their best interest. This sense of connection with the government could also contribute to increased trust among citizens. However, this study found no significant correlation between citizens’ use of social media for government purposes and their level of trust in the government.[[74]](#footnote-77)

There is a significant gap in research on the factors that create trust and result in the successful adoption of e-government services. Very few studies have addressed the impact of trust on satisfaction, continued usage intention, and successful e-government adoption.[[75]](#footnote-78) This research highlights that trust in e-government can be influenced by various factors, including gender, education, perceived risk, and the expectations and beliefs of citizens. 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 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.[[76]](#footnote-79)

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.[[77]](#footnote-80) Government agencies must acquire and advertise features that increase citizens’ perceptions of the site’s trustworthiness as well.[[78]](#footnote-81)

High versus low trust did not affect enforced tax compliance under conditions of low power. There was, however, a significant negative interaction between trust and power. In 13 countries in which power reduced voluntary compliance, whereas in the remaining 31 countries, the level of power showed no significant effect.[[79]](#footnote-82)

1. Special thanks to Arie Balaban Danlielle Ben Arie … [↑](#footnote-ref-1)
2. Porat, Ariel, and Lior Jacob Strahilevitz. "*Personalizing default rules and disclosure with big data*." Mich. L. Rev*.* 112 (2013): 1417. [↑](#footnote-ref-2)
3. 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. (2019). Managemenit t Culture and Surveillance. Seattle UL Rev., **43** 631. [↑](#footnote-ref-3)
4. Aronson, Feldman Lobel Normative Framework for Data Driven Trust [↑](#footnote-ref-4)
5. For the general problem of enforcement, focusing on the wrong place, see Feldman, Yuval, and Yotam Kaplan. "Ethical Blind Spots & Regulatory Traps: On Distorted Regulatory Incentives, Behavioral Ethics & Legal Design." *Law and Economics of Regulation*. Cham: Springer International Publishing, 2021. 37-54. [↑](#footnote-ref-6)
6. 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. [↑](#footnote-ref-7)
7. 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. [↑](#footnote-ref-8)
8. Anaman, Prince Dacosta, and Ibrahim Anyass Ahmed. "*Taxation within the transport sector: A ride-hailer and sharing economy perspective*." Account and Financial Management Journa*l* 6.10 (2021): 2470-2480. [↑](#footnote-ref-9)
9. 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. [↑](#footnote-ref-10)
10. Akagi, D., Amemiya, M. & Shimada, T. *What do security cameras provide for society? The influence of cameras in public spaces in Japan on perceived neighborhood cohesion and trust*. J Exp Criminol 18, 129–147 (2022). [↑](#footnote-ref-11)
11. Chater, N. & Loewenstein, G. (in press). The i-frame and the s-frame: *How focusing on individual-level solutions has led behavioral public policy astray.* Behavioral and Brain Sciences*.* DOI: [https://doi.org/10.1017&am](https://doi.org/10.1017%26am) [↑](#footnote-ref-12)
12. Aronson et al supra note, on file with author [↑](#footnote-ref-13)
13. Supra note \_\_\_ [↑](#footnote-ref-14)
14. Ferguson, Andrew Guthrie. “*Big Data and Predictive Reasonable Suspicion*.” U. Pa. L. Rev*.* 163 (2014): 327.‏ [↑](#footnote-ref-15)
15. Zou, Sheng. "*Disenchanting trust: Instrumental reason, algorithmic governance, and China’s emerging Social Credit System*." Media and Communication 9.2 (2021): 140-149. [↑](#footnote-ref-16)
16. Zou, Sheng (n. 16). [↑](#footnote-ref-17)
17. Wong, K. L. X., & Dobson, A. S. (2019) "*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), 220-232. <https://doi.org/10.1177/2059436419856090> [↑](#footnote-ref-18)
18. Kostka, G. (2019). *China’s social credit systems and public opinion: Explaining high levels of approval*. New Media & Society, 21(7), 1565-1593. <https://doi.org/10.1177/1461444819826402> [↑](#footnote-ref-19)
19. Zou, Sheng. "*Disenchanting trust: Instrumental reason, algorithmic governance, and China’s emerging Social Credit System*." Media and Communication 9.2 (2021): 140-149. [↑](#footnote-ref-20)
20. Angèle Christin, *From Daguerreotypes to Algorithms: Machines, Expertise, and Three Forms of Objectivity*, 46 ACM Computers & Soc’y 27, 27–28 (2016). [↑](#footnote-ref-21)
21. Julie E. Cohen, *What Privacy Is For*, 126 Harv. L. Rev. 1904, 1920 (2013). [↑](#footnote-ref-22)
22. For other definitions of big data, *see* David Lazer & Jason Radford, *Data ex*

*Machina: Introduction to Big Data*, 43 Ann. Rev. Soc.19,19 (2017) (emphasizing the context dependence of any definition of big data);Viktor Mayer-Schönberger & Kenneth Cukier, Big Data: A Revolution That Will Transform How We Live, Work, and Think 2–3 (2013). [↑](#footnote-ref-23)
23. Andrew V. Papachristos, David M. Hureau & Anthony A. Braga, *The Corner and the Crew: The Influence of Geography and Social Networks on Gang Violence*, 78 Am. Soc. Rev. 417, 418, 425 (2013) (Offering a network model that predicts the identity of individuals most likely to participate in gang violence). [↑](#footnote-ref-24)
24. Walter L. Perry, Brian McInnis, Carter C. Price, Susan C. Smith & John S. Hollywood, *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations* 13 (2013). [↑](#footnote-ref-25)
25. Ayal, Shahar, et al. "Three principles to REVISE people’s unethical behavior." *Perspectives on Psychological Science* 10.6 (2015): 738-741. [↑](#footnote-ref-26)
26. *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): 4. [↑](#footnote-ref-27)
27. Banaji, Mahzarin R., and Anthony G. Greenwald. *Blindspot: Hidden biases of good people*. Bantam, 2016., at 10–11. [↑](#footnote-ref-28)
28. Yuval Feldman and Yotam Kaplan "*Big Data and bounded ethicality*." Cornell JL & Pub. Pol׳y 29 (2019): 39. [↑](#footnote-ref-29)
29. The more common term is experimental legislation, *see* Sofia Ranchordas, *The Whys and Woes of Experimental Legislation*, 1 Theory & Prac. Legis. 415, 415 (2013), but the term experimental *regulation* is also mentioned frequently and fits under the same analytical framework, *Id*. at 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, *Id.* at 417. [↑](#footnote-ref-30)
30. Ferguson, *supra* note )n 14). [↑](#footnote-ref-31)
31. Richard Berk, *Balancing the Costs of Forecasting Errors in Parole Decisions*, 74 Alb. L. Rev. 1071, 1074 (2010) (discussing the use of historical data to identify future offenders). [↑](#footnote-ref-32)
32. Brayne, *supra* note **Error! Bookmark not defined.**, at 993. [↑](#footnote-ref-33)
33. Brayne, *supra* note **Error! Bookmark not defined.**, at992. [↑](#footnote-ref-34)
34. Feldman 2018, supra note .. [↑](#footnote-ref-35)
35. Nancy Chi Cantalupo & William C. Kidder, *A Systematic Look at a Serial Problem: Sexual Harassment of Students by University Faculty*, 2018 Utah L. Rev. 671, 671–72 (2018). [↑](#footnote-ref-36)
36. *Id.* at 705. [↑](#footnote-ref-37)
37. *Id.* at 715. [↑](#footnote-ref-38)
38. *Id.* [↑](#footnote-ref-39)
39. *Id.* at 728. [↑](#footnote-ref-40)
40. James Jacobs & Tamara Crepet, *The Expanding Scope, Use, and Availability of Criminal Records*, 11 N.Y.U. J. Legis. & Pub. Pol’y 177, 181–88 (2008). [↑](#footnote-ref-41)
41. Supra note [↑](#footnote-ref-42)
42. *Id.* [↑](#footnote-ref-43)
43. Candice L. Kline, *Security Theater and Database-Driven Information Markets: A Case for an Omnibus U.S. Data Privacy Statute*, 39 U. Tol. L. Rev. 443, 447 (2008); Sam Kamin, *The Private Is Public: The Relevance of Private Actors in Defining the Fourth Amendment*, 46 B.C. L. Rev. 83, 125–27 (2004) (discussing databases that retailers compile in order to store consumer information). [↑](#footnote-ref-44)
44. Haugh, *supra* note **Error! Bookmark not defined.**, at 712, 736. [↑](#footnote-ref-45)
45. 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 (Mar. 22, 2016), <https://www.bloomberg.com/news/articles/2016-03-22/credit-suisse-cia-funded-palantir-build-joint-compliance-firm>. [↑](#footnote-ref-46)
46. Ben-Shahar, Omri, and Ariel Porat. *Personalized Law: Different rules for different people*. Oxford University Press, 2021. [↑](#footnote-ref-47)
47. Ranchordas, Sofia, *Empathy in the Digital Administrative State* (October 20, 2021). Duke Law Journal, 2022, Available at SSRN: [https://ssrn.com/abstract=](https://ssrn.com/abstract%3D) [↑](#footnote-ref-48)
48. *See* Brad Brown, Charles Roxburgh, Jacques Bughin, James Manyika, Michael Chui & Richard Dobbs, *Big Data: The Next Frontier for Innovation, Competition, and Productivity* 85 (2011) (describing police practices in using cellphone information). Ferguson, *supra* note )n 14). [↑](#footnote-ref-49)
49. Matt Burns, *Leaked Palantir Doc Reveals Uses, Specific Functions and Key Clients*, TechCrunch (Jan. 11, 2015), <https://techcrunch.com/2015/01/11/leaked-palantir-doc-reveals-uses-specific-functions-and-key-clients/>. [↑](#footnote-ref-50)
50. *Id.* [↑](#footnote-ref-51)
51. Kim A. Taipale, *Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data*, 5 Colum. Sci. & Tech. L. Rev. 1, 14–15 (2003) (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). [↑](#footnote-ref-52)
52. Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1089 (2002) (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). [↑](#footnote-ref-53)
53. Ferguson, *supra* note )n 14), at 330 (evaluating the constitutionality of the use of big data analytics as a basis for police searches and seizures). [↑](#footnote-ref-54)
54. Solon Barocas & Andrew D. Selbst, *Big Data’s Disparate Impact*, 104 Cal. L. Rev. 671, (2016) on the importance of the data on which the algorithms are being paid. [↑](#footnote-ref-55)
55. Yeung, Karen. "*Algorithmic regulation: A critical interrogation*." Regulation & governance 12.4 (2018): 505-523. [↑](#footnote-ref-56)
56. Bennett Moses, Lyria, and Janet Chan. "*Algorithmic prediction in policing: assumptions, evaluation, and accountability*." Policing and Society 28.7 (2018): 806-822.‏ [↑](#footnote-ref-57)
57. Moy, Laura M. "*A Taxonomy of Police Technology's Racial Inequity Proble*ms." U. Ill. L. Rev*.* (2021): 139.‏ [↑](#footnote-ref-58)
58. Lee, Min Kyung. "*Understanding perception of algorithmic decisions: Fairness, trust, and emotion in response to algorithmic management*." Big Data & Society 5.1 (2018): 2053951718756684.‏ [↑](#footnote-ref-59)
59. Chan, Janet, and Lyria Bennett Moses. "*Making sense of big data for security*." The British journal of criminology 57.2 (2017): 299-319.‏ [↑](#footnote-ref-60)
60. Governments use technological Surveillance as a substitute for trusting people. [↑](#footnote-ref-61)
61. Ferguson, *supra* note )n 14), at 327.‏ [↑](#footnote-ref-62)
62. Warkentin, Merrill, et al. "*Encouraging citizen adoption of e-government by building trust*." Electronic markets 12.3 (2002): 157-162.‏ [↑](#footnote-ref-63)
63. 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.‏ [↑](#footnote-ref-64)
64. 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.‏ [↑](#footnote-ref-65)
65. E.g. Berk, Richard A. "*Artificial intelligence, predictive policing, and risk assessment for law enforcement.*" Annual Review of Criminology 4 (2021): 209-237. [↑](#footnote-ref-66)
66. Welch, Eric W., and Charles C. Hinnant. "*Internet use, transparency, and interactivity effects on trust in government*." 36th Annual Hawaii International Conference on System Sciences, 2003. Proceedings of the. IEEE, 2003.‏ [↑](#footnote-ref-67)
67. 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.‏ [↑](#footnote-ref-68)
68. Bennett Moses, Lyria, and Janet Chan. "*Algorithmic prediction in policing: assumptions, evaluation, and accountability*." Policing and Society 28.7 (2018): 806-822.‏ [↑](#footnote-ref-69)
69. Paul Brezina, 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." SSRN Electronic Journal (2021). [↑](#footnote-ref-72)
70. *Id.* [↑](#footnote-ref-73)
71. Kim, Soonhee, and Jooho Lee. *"E‐participation, transparency, and trust in local government.*" Public Administration Review 72.6 (2012): 819-828.‏ [↑](#footnote-ref-74)
72. *Id.* [↑](#footnote-ref-75)
73. *Id.* [↑](#footnote-ref-76)
74. Song, Changsoo, and Jooho Lee. "*Citizens' use of social media in government, perceived transparency, and trust in government*." \_Public Performance & Management Review\_ 39.2 (2016): 430-453.‏ [↑](#footnote-ref-77)
75. 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.‏ [↑](#footnote-ref-78)
76. *Alzahrani, Latifa, Wafi Al-Karaghouli, and Weerakkody*. (n 80). [↑](#footnote-ref-79)
77. Bélanger, France, and Lemuria Carter. "*Trust and risk in e-government adoption*." The journal of strategic information system*s* 17.2 (2008): 165-176.‏ [↑](#footnote-ref-80)
78. *Bélanger, France, and* *Carter*.(n 82) [↑](#footnote-ref-81)
79. Batrancea, Larissa, et al. "*Trust and power as determinants of tax compliance across 44 nations*." Journal of Economic Psychology 74 (2019): 102191.‏ [↑](#footnote-ref-82)