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

Contents

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

[Introduction 1](#_Toc168483575)

[The Monitoring Everything Challenge 2](#_Toc168483576)

[Technology as a Way to Enhance Communication Between People and the 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 will focus on understanding whether technology could be used to enhance non-coercive compliance by creating better reputational mechanisms and better technological nudges. The usage of technology, discussed in this chapter, will focus on two main aspects. First, the ability to monitor and enforce with more limited effect on crowding out. Second, whether technology could allow us to know which part population could be trusted to engage voluntarily. It should be said upfront that this second goal, while might be seen immediately to the reader as mimicking the Chiness Social Credit initiative, the focus here on technology was much different as it tried to allow the state to control people's social behavior. In this book, the focus on technology is related to the reverse perspective where we are looking for ways through which the state could become less coercive and more trusting towards more people.

Generally, speaking the involvement of technology could go in both directions. On one hand one can say that if we can use monitoring technology is being improved we don’t need so much the goodwill of the people to cooperate intrinsically, it is enough that we give people clear instructions and follow how they behave, thus, together with research about personalization,[[2]](#footnote-2) and technology-based enforcement,[[3]](#footnote-3) could possibly reduce some of the need for reliance on the goodwill of people. This could then potentially facilitate more types of cooperation by people, reducing or eliminating the need for state monitoring or the use of sanctions as part of a command-and-control approach.

Research in areas such as algorithmic management shows some mixed signals regarding the potential crowding out effect of rating and monitoring procedures which create a challenge for the promise of technology to enhance intrinsically driven compliance, but rather might at most reduce the need for state-imposed sanction. Hence, we will also examine in this chapter the potential pitfalls of using technology as a substitute for state enforcement. Thus, while technology can indeed replace some more noticeable enforcement attempts, much of the current research tends to view technology as alienating people.

On the other hand, the reliance on technology could be used to take a more trusting approach in which the state can feel secure enough to give people as much discretion as possible, with some ability to avoid direct monitoring interaction with government officials. It carries the ability to allow the state to enjoy both worlds while using some personalized data on past behavior, as discussed in the work with Aronson and Lobel on trust-based regulation, they can allow more and more people great freedom without harming those who are less deserving of this trust[[4]](#footnote-4)

## The Monitoring Everything Challenge

As mentioned above, the big challenge in the usage of technology is whether we can get to a monitoring level that will make the need to trust people unnecessary simply because we can monitor almost every action of individuals. As we have argued this new ability by the state could go both ways, as either pushing in the direction of perfect monitoring, preventing the need for trust, or allowing the state to move forward with trusting the people whose past behavior justifies it. At the same time, we should also take into our normative analysis that there are no such things, at least not just yet as perfect technological monitoring. This is true on a few aspects: first, we are not being monitored all the time. Not only that, but sometimes in the contexts where we need people to comply the most, it is much harder for the state to monitor without interfering with one’s privacy. 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 spread happened. Thus, it was much easier for the state to monitor the area in which voluntary compliance is the least problematic because epidemiologically it is less dangerous. Close spaces where more of the virus transfer could happen are much harder for the state to enforce, is much easier such contexts.[[5]](#footnote-5) The need for voluntary compliance is of course greater in the areas were enforcement in general and technological in particular is the hardest.

One of the cautions we put forward regarding voluntary compliance is related to the need to convince those people who weren’t originally supportive of the government policy, to behave in a trustworthy way. This process might be less supportive of people’s autonomy and should be compared to the damage to autonomy that is associated with algorithmic regulation. Hence the comparison between the two approaches should be between what approach is more harmful to the peoples’ feeling of choosing whether they want to freely choose to comply with state’s laws and regulations. The comparison becomes even more complicated as the usage of technology can help us determine also using big data approaches, the identity of people who might not even need convincing as their behavior should affect the choice between the technological approach and the trust-based approach. As for those people, trust-based regulations a concept which was explained in Chapter 4 in more detail, will not require any process of internalization and hence for them, the usage of technology is far less desirable.

In this chapter, we will focus on a few elements of the interaction between technology and voluntary compliance:

1. Technology affects the interaction between people and the state, by that reducing the level of flexibility that exists in human decision-making, where cutting corners might be more prevalent, relative to situations, where technology is being used.
2. Technology has improved the level of enforcement making the need for governments to trust peoples’ voluntary compliance. It also allows the government the ability to differentiate between people based on their past behavior (which is relevant also for the next argument).
3. Technology is improving the level of personalization in regulation, creating a more personalized and differentiated approach to regulation and by that making it easier for people to feel that the regulation is aligned with their personal preferences.
4. Technology is increasing the ability to use incentives thus, creating at least an opportunity for incentivized voluntary compliance, which might in the long run become internalized voluntary compliance.

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

Extensive research in the area of technology and governance has focused on the area of E-government is a relatively new mode of citizen-to-government contact founded in information and communications technologies, based on governments’ trust in their citizens and how citizens view the government as a function of their technological experience when working with the government.[[6]](#footnote-6) Findings suggest, that although e-government may help improve citizens’ confidence in the future performance of the agency experienced, it does not yet lead to greater satisfaction with an agency interaction, nor does it correlate with greater generalized trust in the federal government overall.[[7]](#footnote-7) To the best of our knowledge most of the current research in these areas, focus on ethical issues related to technological monitoring and satisfaction of citizens from the better efficiency of technological services governments are offering.

## Technology – More Monitoring, Less Trust?

In many ways, much of the role of law and technology focuses on questions of trust and the ability of people to trust technology. On one hand, as suggested in the introduction, technology is likely to reduce the leverage that people must cheat, hence reducing the need for government to trust people’s compliance. A classical example, of how technology improves monitoring is the usage of cash. From a tax evasion perspective, the cash economy is the hardest to monitor. Various means are being used to replace cash with more traceable ways (not accounting for advancements such as Bitcoin, which are even more evasive to authorities).

For example, relative to taxi drivers, uber drivers or taxi drivers using various apps, are far less likely to cheat the tax authority when their payments are being received via the app. Similarly renting which is done via booking and abb is less likely to be subject to tax evasion.[[8]](#footnote-8) Furthermore, even in services such as Airbnb Uber, and Lift. At the same time, these services are not only reducing the ability to evade taxes but also to understand from the side of the public, who can they trust based on various reputation and reporting systems.[[9]](#footnote-9)

## Cameras in Public Spaces and Trust

What technology is trying to achieve is to make it easier for states to trust people, not because they trust them, but because there is an algorithm that suggests they can be more laid back in enforcement, given 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 bar so that smaller misdemeanors will be tolerated? The anti-cash revolution might change the need for trust in taxation. Did it work so far? Do we prefer nudges to contact tracing apps and how about epidemiological interviews with people who got infected?[[10]](#footnote-10)

## Regulating Situations vs. Regulating People

The new paper by Chapter and Lowenstein[[11]](#footnote-11) and others might support the view that technological changes could replace some of the need to change intrinsic motivation. When they focus on the responsibility of the corporation of climate change they also suggest that we need to focus on technology which will reduce some of the responsibility from the shoulders of the people themselves.

The attempt of this book to find what is the intrinsic motivation of people is quite limited. Technology could be seen as the kind of change that might replace individual responsibility and behavioral change.

In other words, are technologies a replacement for an intrinsic change or a way to enhance it because states will not need to think about whom to trust and can focus more on going to the next level by focusing on things like quality of compliance, discussed in the first chapter.

## Proportionality and Behavioral Big data

In a joint work with Ori Aronson and Orly Lobel,[[12]](#footnote-12) we are focusing on the constitutionality of differentiating between people based on their past behavior. Data-based trust in groups and individuals. The computational powers of algorithms present an opportunity to shift from blinding certain information for privacy and equality concerns to a new paradigm of fairness through awareness. The ability of AI to discern patterns from proxies to identity carries vast potential but also deep risks. In that paper, we explore the ethical and regulatory challenges of algorithmic data-driven trust methods that enhance trust in individuals for regulatory purposes. These methods are relevant in diverse regulatory contexts. They involve assessing trustworthiness at both individual and group levels. Machine learning can aggregate data to create individual "compliance scores," raising questions about their societal acceptance. Additionally, it poses concerns about norm violations affecting one's overall trustworthiness score, encompassing accuracy, legality, and moral considerations. Group-level trust relies on data linking compliance to group affiliations, but this can reinforce biases and class disparities, especially for marginalized groups.

In our joint work,[[13]](#footnote-13) we address the gap in existing big data research by examining the feasibility and desirability of utilizing big data for regulatory decision-making. In the context of trust-based regulation, it explores the challenge of identifying trustworthy individuals within the public. Specifically, it delves into the ability to predict and assess public cooperation, as demonstrated during the early days of the COVID-19 pandemic when governments had to decide whether to rely on public trust for compliance with safety measures. Big data offers the potential to distinguish individuals and groups accurately, enabling more precise predictions of voluntary cooperation in trust-based regulation. These questions hold significance in the design of less coercive regulatory systems, given the reciprocal nature of trust, where placing trust in individuals can foster increased trustworthiness. While the idea of suspecting individuals might intuitively lead to changes in behavior, there is less empirical research on this aspect.

The Fourth Amendment protects individuals from unreasonable police searches and seizures. big data information will impact all major aspects of traditional policing, including stopping and frisking. The more data known or discovered about a particular suspect, the easier it is to justify a stop based on reasonable suspicion. According to the article, there can be problems with using big data on suspects, besides leading to mistakes and being a violation of the right to privacy, big data can also overwhelm officers and interfere with the determination of who should be stopped for suspected criminal activity.[[14]](#footnote-14)

We further develop some ethical considerations in data-driven trust regulation, and explore the ethics of differentiated lawmaking and regulation, with a focus on data-based trust regulation. We outline key ethical considerations in this context. For example, what is the meaning of statistical trust, what effect sizes should justify a policy change, and what level of correlation could be seen as predictive enough to allow different treatments? What policy purposes justify predictions, and security concerns, or provide more efficient ways to collect taxes? The proportionality doctrine in constitutional law, suggests that we are allowed to engage in activities that are more likely to infringe on peoples’ rights when the goal, policymakers attempt to achieve is greater.

Overall, the work with Aronson and Lobel, highlights key ethical issues in differentiated lawmaking and regulation, focusing on data-driven trust regulation. Navigating these complexities is essential for policymakers and regulators to promote fairness, transparency, and equity in our data-driven world. In that work we examine real-world examples, such as predictive systems for identifying likely harassers and cases like COMPASS, to gain insights into the ethical and regulatory challenges of algorithmic data-driven trust mechanisms.

This discussion is a good way to move to the country that is most associated with data-driven regulation, especially in ethical contexts – China.

## China's social credit system- trustworthiness

China's Social Credit System (SCS) has sparked international fears of an Orwellian techno-dystopia. Research on China examined the expansion of algorithmic rating into daily life.[[15]](#footnote-15) Indeed, China's plan to build a Social Credit System has evoked fear internationally of an Orwellian techno dystopia. The paper argues that the SCS is an epitome of the quantification of the social disenchants and flattens moral values such as trust and trustworthiness.[[16]](#footnote-16) It seems from current research that China is conducting a pilot of its expansive Social Credit System (SCS) in select cities,[[17]](#footnote-17) aiming to merge financial credit scores with broader societal assessments. The SCS employs a reward and punishment system, incentivizing adherence to government values and penalizing deviations. It addresses trust and integrity issues in Chinese society amidst 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 Social Credit Systems (SCS). A survey conducted through online platforms revealed that four out of five respondents use commercial SCS, while only 7% were aware of local government-run systems.[[18]](#footnote-18)

According to the survey, a majority (59%) believe the central government should manage a nationwide social media surveillance system. Trust in political institutions varies, favoring the central government over local ones In summary, according to this paper, China's citizens perceive SCS as a means to enhance life quality and bridge institutional gaps in a data-driven governance landscape.

Research in China examined the expansion of algorithmic rating into daily life through the Frankfurt School's critique of instrumental reason .[[19]](#footnote-19) Zou's research is a good example of the problem in technological monitoring in general as it suggests that the way algorithmic systems measure trust exemplifies the increasing role of technology and instrumental reason in society. This approach prioritizes the identification of patterns and correlations in data while neglecting the traditional methods of scientific verification. As a result, the emphasis shifts from human relationships to technical efficiency, reducing trust to mere confidence in technology and discouraging risk-taking behavior. The Social Credit System in China, which combines economic and social behavior, is a prime example of this growing trend of technologized governance. However, the author argues that cultivating genuine trust demands a different logic that goes beyond mere instrumentality and resists the urge to quantify everything excessively.

## Big Data and Voluntary Compliance

Following the previous discussion on China’s social credit approach, in another joint project this time with Yotam Kaplan we have examined ways to use big data in manners which are less harmful to people’s autonomy and privacy. Our research explores the shift from personalization to a situational approach in the context of big data and bounded ethicality.

Recent years have seen a remarkable rise in big data's use for predictive decision-making across diverse sectors like finance, healthcare, and law enforcement,[[20]](#footnote-20) As Julie Cohen points out,[[21]](#footnote-21) 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 requires immense datasets, often in petabytes, integrating information from various sources.[[22]](#footnote-22) Current applications include spam and fraud detection, credit scoring, insurance pricing, and data-driven law enforcement, such as predicting gun violence,[[23]](#footnote-23) and serious crimes.[[24]](#footnote-24)

Utilizing big data for predictive regulation allows regulators to preemptively engage with potential wrongdoers, issuing alerts before misconduct occurs. This data-driven approach effectively tackles ethical challenges. Another important concept we develop is targeted regulation, where Data-driven law enforcement enables regulators to focus on specific risks and behaviors rather than random enforcement. This targeted approach is essential to counter ethical numbing and improve ethical deliberation., finally we also discuss the concept of Tailored Regulation, where Data-driven law enforcement aids in choosing the right regulatory tools by providing insights into specific cases of misconduct. Big data analysis helps predict the effectiveness of ethical interventions based on past transgressors' histories and situational characteristics.

While the focus of the work with Kaplan, discussed above was on the context of bounded ethicality, this newfound ability is crucial for overcoming the danger of ethical numbing discussed above.[[25]](#footnote-25) To improve ethical deliberation, regulatory intervention must be targeted and specific, rather than general and broad. For example, ethical alerts are effective only if they are targeted and rare, rather than routine and constant.[[26]](#footnote-26) If everyone is randomly bombarded with ethical messages, those messages will quickly lose their meaning and impact.[[27]](#footnote-27) Big data analysis offers a crucial advantage here, as it facilitates a regulatory scheme that only becomes operative when analysis of background information indicates that its involvement is necessary.

## Tailored Regulation

Data-driven law enforcement can provide tools to overcome the challenge of choosing the right tools to effectively trigger deliberation and address bounded ethicality. This will be crucial in determining the most appropriate legal response, according to the nature of the ethical bias preventing candid deliberation.

Indeed, big data analysis can provide a plethora of information on specific cases of misconduct, in a way that will enable regulators to devise the most appropriate regulatory response. Situations in which many of the likely transgressors are first-time offenders are more likely to be characterized by ethical blind spots relative to situations in which the transgressor is a repeat protagonist, making the possibility of unfamiliarity with the ethical problem of the behavior less likely. Moreover, using big data, we can also learn the transgression history of the most common transgressors and recognize the most suitable ethical nudges. Essentially, the history of the violations of the typical transgressor could be used to generate better predictions not just of the situational characteristics where we expect increased levels of unethical behavior, but also of the characteristics of the interventions that will be effective, based on their past efficacy across different situations.[[28]](#footnote-28)

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-29) Randomized content can use the protocols of experimental design and their varying effects using big data analysis. After randomized messages are deployed, statistical analysis can provide insights into the effectiveness of each one.

## Integrated Datasets

Another aspect that Kaplan and I discuss is the integration of data from previously separate institutional sources.[[30]](#footnote-30) 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-31) The move towards *big* data entails the merging of information from multiple sources and its systematic and integrated analysis.[[32]](#footnote-32) Such an integrated system allows users to track disparate data points in relation to one another and study correlations between data points originating in different datasets.

Kaplan and I demonstrate in that paper the recent move towards big data law enforcement entails a departure from this tradition, in favor of the inclusion of information on those with no prior contact with law enforcement authorities.[[33]](#footnote-33) Policymakers can also now regulate people with no prior encounters with the law, which is crucial considering the understanding that bounded ethicality is far more common, as discussed in the law of good people.[[34]](#footnote-34)

Such an integrated approach can be illustrated through recent work by Cantalupo & Kidder, who utilized the latest advances in data availability to analyze and categorize sexual harassment by university faculty members.[[35]](#footnote-35) They use a database drawn from media reports,[[36]](#footnote-36) federal civil rights investigations by the United States Departments of Education and Justice,[[37]](#footnote-37) lawsuits by students alleging sexual harassment,[[38]](#footnote-38) and lawsuits by tenure-track faculty fired for sexual harassment.[[39]](#footnote-39) More generally, many types of databases are now available for integrated, data-driven law enforcement; any dataset documenting and recording misconduct or dispute can be a relevant source of information.[[40]](#footnote-40)

First, databases currently used and maintained by law enforcement agencies can prove helpful in identifying patterns of unethical behavior. Existing law enforcement datasets have grown increasingly rich and detailed, now offering data points measured in the trillions, even before the transition to integrated 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, this currently available data can be crucial in identifying and characterizing the precise details of situations that foster unethical conduct.

According to Jacobs and Crepet[[41]](#footnote-41), private commercial actors may also maintain databases that could prove useful for our purposes. Thus, financial institutions keep extensive records, directly and indirectly documenting the actions, preferences, and behavior of both employees and consumers.[[42]](#footnote-42) Similar datasets are maintained and used by retailers, pharmaceutical companies, and technology firms.[[43]](#footnote-43) Some private companies, especially in financial markets, are already implementing situational regulation of their employees. For example, JP Morgan Chase provides ethical reminders to employees, warning them when they are approaching the limits of legitimate business practices. Such warnings are based on “predictive monitoring” algorithms and attempt to prevent wrongdoing before it occurs.[[44]](#footnote-44) This type of mechanism, which is based on big data analysis, is now being adopted by other financial institutions.[[45]](#footnote-45)

## The Personalized Law Approach

Ben Shachar and Porat’s influential book on personalized law,[[46]](#footnote-46) sees technology with a special focus on big data as a solution to the fact that peoples’ preferences differ from each other across many legal domains. In their book, they demonstrate how using big data analytics the law could provide more tailored solutions to numerous factors that can predict peoples’ preferences and align them with various fairness constraints. While in their book, the notion of people’s ethics and willingness to cooperate is not mentioned, it is worth examining how their approach could justify a situation, where people’s past cooperation will affect how much trust should the government place in their declarations to cooperate voluntarily.

The notion of personalization could also be embedded in various technologies for example regarding the type of a pledge the individual will need to sign, changing the text, and alternating the opting out to allow for omissions. Tax authorities could learn what practices have worked to enhance ethicality for people who share the same characteristics as the individual. When more and more of the individual interaction with the government is through the digital platform personalization which will focus on enhancing ethicality rather than attempting to learn their preferences and create a suitable legal framework.

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

Another important aspect of the ability of technology to enhance voluntary compliance is the role of empathy, which is somewhat missing when algorithms are making policy decisions, regarding people. Sofia Richards writes that Making mistakes is a fundamental human trait, especially when dealing with complex government forms like tax returns and benefit applications. However, the capacity for forgiveness of these errors is diminishing due to the increasing digitization and automation of government services. She argues that empathy has played a controversial yet crucial role in helping public authorities balance administrative values with citizens' needs, particularly benefiting vulnerable groups such as disabled individuals, seniors, minorities, and those with low incomes. In the digital administrative state, the erosion of empathy poses a risk to the ability of vulnerable citizens to access their rights through the digital bureaucracy. Her research contends 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 advocate for emotional-based exceptions or individualized justice but rather proposes strategies to humanize digital governance and automated decision-making through a comprehensive grasp of citizens' requirements. Ranchlands examines the role of empathy within the digital administrative state on two fronts: firstly, it maintains that administrative empathy can address certain deficiencies of digital bureaucracy by acknowledging citizens' diverse competencies and needs, necessitating the redesign of application forms, governmental platforms, algorithms, and support mechanisms. Secondly, empathy should function post-decision as a means of humanizing administrative decision-making. Drawing upon comparative instances of empathic practices in the United States, the Netherlands, Estonia, and France, Richards 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, working in the area of algorithmic enforcement is that the practice of using big data is already deeply entrenched in existing law enforcement procedures.[[48]](#footnote-48) To give one example of this trend, consider the case of Palantir Technologies, a private software company specializing in big data analytics.[[49]](#footnote-49) Palantir, founded in 2004, is just one of the major big data platforms currently used by law enforcers in the United States.[[50]](#footnote-50) 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-51)

The argument Kaplan and I made is that the prevalence of data-driven law enforcement has raised important legitimacy concerns. Mainly, commentators have voiced objections to this emerging form of law enforcement based on privacy and autonomy concerns,[[52]](#footnote-52) arguing that law enforcement based on big data may violate citizens’ Fourth Amendment rights.[[53]](#footnote-53) Many studies have shown that big data analysis by policymakers can perpetuate existing discriminatory patterns by mimicking them.[[54]](#footnote-54) In this chapter, we argue for a reorientation of current practices of big data law enforcement and a rethinking of its goals and operations. We show that if big data law enforcement makes the regulation of bounded ethicality its main goal, as we propose, this can help mitigate some of the legitimate concerns regarding the use of big data analytics by law enforcers. This is true for two main reasons. First, to overcome bounded ethicality, governments do not need to gather information at the personal level. Unlike the use of big data in other contexts, such as the prevention of serious crime, the goal of government intervention is not to single out exceptionally malevolent individuals but to identify the conditions that lead to ethical biases by ordinary people. This means that privacy concerns are somewhat less alarming in this context, as information need not be attached to specific individuals. Similarly, concerns regarding the perpetuation of prejudice and discriminatory practices are less troubling, again because big data analysis is used to produce situational predictions rather than personalized ones.

**Algorithmic Regulation**

With the discussion of the potential of algorithms to help with the trust puzzle by regulators, it is important to acknowledge the increase in research which was already done on algorithmic regulation.[[55]](#footnote-55) Yeung's study examines algorithmic regulation, a form of decision-making that manages risk and alters behavior through continuous data collection and computational analysis. The research classifies these systems as reactive or pre-emptive and provides a taxonomy of eight different forms based on their configuration at three stages: standard setting, information-gathering and monitoring, and sanction and behavioral change. The study explores emerging debates surrounding algorithmic regulation, drawing insights from various disciplines to highlight concerns about its legitimacy. Yeung's descriptive analysis contributes to the understanding of the complex nature and potential implications of algorithmic regulation also in the context of compliance with and without other means of enforcement.

**Algorithmic Policing**

Indeed, the additional studies, that complete the above discussion of algorithmic regulation is algorithmic enforcement, where part of the challenge is to understand whether the current research view is as a mechanism that is less likely to crowd out their compliance motivation. Generally speaking, as will be outlined in the coming paragraph, most studies take the perspective that technology might decrease pubic trust rather than increase it.

For example, concerns have been raised that new police technologies may aggravate existing inequities in policing.[[56]](#footnote-56) For example, police in many cities use predictive policing algorithms to find patterns in data about criminal activity and use those patterns to proactively deploy police to locations where crimes are statistically more likely to occur. However, because the underlying data encodes existing racial inequity in policing, predictive policing may learn and replicate racial bias. A second example is as follows. many police forces use automated face recognition technology to help identify faces captured in photos and videos of crime suspects. 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. Hence current research tries to mitigate such fear by offering various models of equity impact assessment for proposed police technologies.[[57]](#footnote-57)

In another survey, participants thought an algorithm would not be able to discern good candidates because it would lack human intuition and make judgments based on keywords, or ignore qualities that are hard to quantify, which indicates a lower level of trust in this type of task done by algorithm.[[58]](#footnote-58) 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, which will affect the likelihood and extent of impact on the potential 'losers'.[[59]](#footnote-59)

Governments use technological Surveillance as a substitute for trusting people. Surveillance is also a mode of engagement with the world enabling trust, accountability, and eventually responsible humanitarianism. It uses the example of predictive policing to consider the difference between panoptic modes of surveillance and emerging practices of environmental surveillance.[[60]](#footnote-60) Predictive policing involves the claimed ability to 'forecast where and when the next crime or series of crimes will take place'. The appropriate balance between ensuring predictive accuracy and protecting historically disadvantaged groups is a difficult, and subjective one. Existing research worries about the possibility that law enforcement officers will not fully comply with the needed safeguards.[[61]](#footnote-61) Because of the lack of trust by the public, there might be a need to use an independent judicial body to help. Governments can convince citizens that the same rigorous controls that make government handling of traditional tax returns are also transferable to online tax returns.[[62]](#footnote-62)

The survey queried citizens about their experience with, involvement with, and perceptions of e-government.[[63]](#footnote-63) It found among other things that such communication approaches might be seen by people as a way that mostly helps the government.

New York City Police Department switched from old-style policing to one based on predictive analytics to respond to an increased demand for police services. Causing certain groups of people to be regularly suspected based on their risks and threats.[[64]](#footnote-64)

A related problem to the discussion about the lack of trust in academic policing is related to the problem of transparency which is sometimes lacking in AI driven-policing.[[65]](#footnote-65)

**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 stronger citizens believe that government websites provide reliable information, the greater their trust in government.[[66]](#footnote-66)

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 holds promise for improved delivery of many types of public services. The paper continues to argue that federal government websites are related to increased perceptions of the transparency of government.[[67]](#footnote-67) Most prediction software focuses on place rather than people, but it remains important to understand the impossibility of neutrality concerning the existence of historic discrimination in historical data.[[68]](#footnote-68)

The ability to calculate (whether accurately or inaccurately) the geo-spatial distribution of future crime itself changes the context in which police strategies are formulated. Some predictive programs are primarily about mobilizing police patrols to particular blocks based on predictive analytics, not about attempting to understand the causes of crime in a particular area. Police resistance may be a barrier to the successful implementation of predictive policing. Hot spots must be small enough to patrol effectively and there must not be too many of them. There is credible empirical evidence that the use of hot spot policing can lead to lower crime levels.[[69]](#footnote-69)

According to the article, the findings of the research could be interpreted as a sign that too strict enforcement under the form of audit rates and severe fines may result in reactance and resistance-provoking compliance.

According to the article, Successful implementation of e-audits requires broad acceptance from taxpayers and tax auditors. Audit certainty significantly increases trust in the tax authorities, with no significant effect on perceived power. The article suggests that trust leads to voluntary compliance and power to enforce compliance, but that a fair amount of power of tax authorities still must be present.[[70]](#footnote-70)

Taxpayers who already display high trust in tax authorities are more likely to endorse e-audits and react to them with higher increases in trust. Tax auditors react negatively to the same feature that made audit certainty attractive to taxpayers, namely audit certainty.[[71]](#footnote-71) 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.[[72]](#footnote-72) E-participants who receive quality feedback and responses from government officials are likely to perceive that they have useful policy information that helps better understand government agencies and community issues. The quality of government response to citizen participants can help boost their self-esteem.[[73]](#footnote-73) In that regard, a recent study found that if citizens believe e-government is more transparent, they are more likely to return to the site.[[74]](#footnote-74)

Increased communication from the government about its actions taken in the best interest of citizens can enhance the relationship between the government and its people. This sense of connection with the government might also contribute to increased trust among citizens. However, this study found no significant correlation between citizens' use of social media in government and their level of trust in the government.[[75]](#footnote-75)

Research on the antecedents of trust that lead to successful e-government service adoption has a notable gap. According to the paper, very few studies have addressed the impact of trust on satisfaction, continued usage intention, and successful e-government adoption.[[76]](#footnote-76) This research points out that trust in e-government is affected by several factors, such as gender, education, risk, and citizens' expectations and beliefs. The accuracy, completeness, and timeliness of information on government websites, as well as the reliability and accessibility of the system, are factors that influence citizens' trust.

More research on the relationship between trust and technology suggests that Citizens’ level of trust in the government increases when they are informed about the actions and processes of the government. Having the users participate in the process, as well as consulting them for their views is an imperative approach to creating trust.[[77]](#footnote-77)

If government agencies expect citizens to provide sensitive information and complete personal transactions online, they must acknowledge and enhance citizens' views concerning the credibility of e-government services.[[78]](#footnote-78) It is imperative that government agencies acquire and advertise features that increase citizens' perceptions of the site's trustworthiness as well.[[79]](#footnote-79)

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 power reduced voluntary compliance, whereas in the remaining 31 countries, power showed no significant effect.[[80]](#footnote-80)

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-5)
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-6)
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-7)
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-8)
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-9)
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-10)
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> [↑](#footnote-ref-11)
12. Aronson et al supra note, on file with author [↑](#footnote-ref-12)
13. Supra note \_\_\_ [↑](#footnote-ref-13)
14. Ferguson, Andrew Guthrie. “*Big Data and Predictive Reasonable Suspicion*.” U. Pa. L. Rev*.* 163 (2014): 327.‏ [↑](#footnote-ref-14)
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-15)
16. Zou, Sheng (n. 16). [↑](#footnote-ref-16)
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-17)
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-18)
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-19)
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-20)
21. Julie E. Cohen, *What Privacy Is For*, 126 Harv. L. Rev. 1904, 1920 (2013). [↑](#footnote-ref-21)
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-22)
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-23)
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-24)
25. Ayal, Shahar, et al. "Three principles to REVISE people’s unethical behavior." *Perspectives on Psychological Science* 10.6 (2015): 738-741. [↑](#footnote-ref-25)
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-26)
27. Banaji, Mahzarin R., and Anthony G. Greenwald. *Blindspot: Hidden biases of good people*. Bantam, 2016., at 10–11. [↑](#footnote-ref-27)
28. Yuval Feldman and Yotam Kaplan "*Big Data and bounded ethicality*." Cornell JL & Pub. Pol׳y 29 (2019): 39. [↑](#footnote-ref-28)
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-29)
30. Ferguson, *supra* note )n 14). [↑](#footnote-ref-30)
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-31)
32. Brayne, *supra* note **Error! Bookmark not defined.**, at 993. [↑](#footnote-ref-32)
33. Brayne, *supra* note **Error! Bookmark not defined.**, at992. [↑](#footnote-ref-33)
34. Feldman 2018, supra note .. [↑](#footnote-ref-34)
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-35)
36. *Id.* at 705. [↑](#footnote-ref-36)
37. *Id.* at 715. [↑](#footnote-ref-37)
38. *Id.* [↑](#footnote-ref-38)
39. *Id.* at 728. [↑](#footnote-ref-39)
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-40)
41. Supra note [↑](#footnote-ref-41)
42. *Id.* [↑](#footnote-ref-42)
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-43)
44. Haugh, *supra* note **Error! Bookmark not defined.**, at 712, 736. [↑](#footnote-ref-44)
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-45)
46. Ben-Shahar, Omri, and Ariel Porat. *Personalized Law: Different rules for different people*. Oxford University Press, 2021. [↑](#footnote-ref-46)
47. Ranchordas, Sofia, *Empathy in the Digital Administrative State* (October 20, 2021). Duke Law Journal, 2022, Available at SSRN: <https://ssrn.com/abstract=> [↑](#footnote-ref-47)
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-48)
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-49)
50. *Id.* [↑](#footnote-ref-50)
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-51)
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-52)
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-53)
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-54)
55. Yeung, Karen. "*Algorithmic regulation: A critical interrogation*." Regulation & governance 12.4 (2018): 505-523. [↑](#footnote-ref-55)
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-56)
57. Moy, Laura M. "*A Taxonomy of Police Technology's Racial Inequity Proble*ms." U. Ill. L. Rev*.* (2021): 139.‏ [↑](#footnote-ref-57)
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-58)
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-59)
60. Governments use technological Surveillance as a substitute for trusting people. [↑](#footnote-ref-60)
61. Ferguson, *supra* note )n 14), at 327.‏ [↑](#footnote-ref-61)
62. Warkentin, Merrill, et al. "*Encouraging citizen adoption of e-government by building trust*." Electronic markets 12.3 (2002): 157-162.‏ [↑](#footnote-ref-62)
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-63)
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-64)
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-65)
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-66)
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-67)
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-68)
69. *Id*. [↑](#footnote-ref-69)
70. 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-70)
71. *Id.* [↑](#footnote-ref-71)
72. Kim, Soonhee, and Jooho Lee. *"E‐participation, transparency, and trust in local government.*" Public Administration Review 72.6 (2012): 819-828.‏ [↑](#footnote-ref-72)
73. *Id.* [↑](#footnote-ref-73)
74. *Id.* [↑](#footnote-ref-74)
75. 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-75)
76. 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-76)
77. *Alzahrani, Latifa, Wafi Al-Karaghouli, and Weerakkody*. (n 80). [↑](#footnote-ref-77)
78. 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-78)
79. *Bélanger, France, and* *Carter*.(n 82) [↑](#footnote-ref-79)
80. Batrancea, Larissa, et al. "*Trust and power as determinants of tax compliance across 44 nations*." Journal of Economic Psychology 74 (2019): 102191.‏ [↑](#footnote-ref-80)