Asia Journal of Management
and Social Science
Vol. 01 / No. 01 / 2023

Legal and Ethical Implications of Multidisplay Surveillance Systems

Muhammad Afzal

COMSATS Institute of Information Technology, Islamabad

Abstract:

This paper delves into the legal and ethical ramifications surrounding the implementation of multidisplay surveillance systems. These systems, characterized by their capacity to monitor multiple environments simultaneously through an array of interconnected displays, raise profound concerns regarding privacy, civil liberties, and the balance between security and individual rights. Drawing upon legal frameworks, ethical principles, and case studies, this study explores the complexities inherent in regulating and governing multidisplay surveillance systems in diverse contexts.

Keywords: *multidisplay surveillance systems, legal implications, ethical implications, privacy, civil liberties, security, regulation*

Introduction:

The advent of multidisplay surveillance systems represents a significant advancement in monitoring capabilities, enabling the simultaneous observation of multiple environments from a centralized control hub. While these systems offer unparalleled surveillance potential for various sectors including law enforcement, public safety, and commercial enterprises, they also pose intricate legal and ethical challenges. This paper aims to dissect the multifaceted nature of these challenges, examining the implications for privacy, civil liberties, and the overarching societal

Legal Implications of Multidisplay Surveillance Systems:

The integration of multidisplay surveillance systems into various sectors has raised profound legal implications, necessitating a careful examination of existing laws and regulations. Firstly, privacy concerns loom large, as these systems have the potential to monitor multiple environments simultaneously, blurring the lines between public and private spaces. Laws governing data collection, storage, and sharing must be scrutinized to ensure that individuals' privacy rights are adequately protected in the face of pervasive surveillance.

Secondly, the Fourth Amendment, which protects against unreasonable searches and seizures, is at the forefront of discussions surrounding multidisplay surveillance. The deployment of these systems, particularly in public spaces, challenges traditional notions of privacy and prompts questions about the scope of governmental authority in conducting surveillance activities. Courts are grappling with the application of Fourth Amendment principles to emerging surveillance technologies, seeking to strike a balance between security interests and individual rights.

Issues related to data retention and access compound the legal complexities of multidisplay surveillance systems. The vast amount of data collected by these systems raises questions about how long data should be stored, who should have access to it, and under what circumstances.

Balancing the need for law enforcement and security agencies to access relevant information with individuals' rights to privacy and due process presents a significant legal challenge in the digital age.

The legal landscape surrounding multidisplay surveillance is further complicated by the proliferation of smart city initiatives and urban monitoring programs. These initiatives often involve the deployment of surveillance technologies on a large scale, raising concerns about mass surveillance, discriminatory practices, and the potential for misuse of collected data. As such, legal frameworks must evolve to address the unique challenges posed by these expansive surveillance systems while safeguarding fundamental rights and freedoms.

Navigating the legal implications of multidisplay surveillance systems requires a nuanced understanding of privacy laws, constitutional rights, and the evolving nature of surveillance technologies. It is imperative that policymakers, lawmakers, and legal scholars engage in robust discussions to develop regulatory frameworks that strike a delicate balance between security imperatives and individual liberties in an increasingly surveilled world.

Privacy Laws and Regulations:

Privacy laws and regulations serve as a crucial framework for addressing the legal implications of multidisplay surveillance systems. At the forefront of these considerations are laws governing data protection and privacy, such as the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) in the United States. These regulations establish principles for the collection, processing, and storage of personal data, imposing obligations on organizations to ensure transparency, consent, and data minimization in their surveillance activities.

Sector-specific regulations play a significant role in shaping the legal landscape of multidisplay surveillance. For instance, in the healthcare sector, the Health Insurance Portability and Accountability Act (HIPAA) in the U.S. sets stringent requirements for the protection of individuals' health information, which extends to surveillance systems used in healthcare facilities. Similarly, financial institutions must comply with regulations like the Payment Card Industry Data Security Standard (PCI DSS), which governs the protection of payment card data, including data captured by surveillance systems in bank branches and ATMs.

In addition to domestic regulations, international agreements and frameworks also influence privacy laws pertaining to multidisplay surveillance. The Council of Europe's Convention 108, for instance, establishes common principles for the protection of individuals with regard to the automatic processing of personal data, providing guidance to member states on safeguarding privacy rights in the context of surveillance technologies. Similarly, the International Principles on the Application of Human Rights to Communications Surveillance, endorsed by the United Nations, outline principles to ensure that surveillance activities comply with human rights standards, including the right to privacy and freedom of expression.

Evolving technologies and surveillance practices necessitate continuous updates to privacy laws and regulations to address emerging threats and challenges. As multidisplay surveillance systems

become more sophisticated, policymakers must consider the implications of artificial intelligence, biometric identification, and predictive analytics on individuals' privacy rights. This requires a proactive approach to legislation and regulatory enforcement, fostering collaboration between government agencies, industry stakeholders, and civil society organizations to develop robust safeguards against potential abuses of surveillance technologies.

Privacy laws and regulations provide a vital framework for addressing the legal implications of multidisplay surveillance systems, offering guidance on data protection, consent, and accountability. By ensuring compliance with these laws, policymakers can uphold individuals' privacy rights while balancing the need for security and public safety in an increasingly surveilled world.

Fourth Amendment Considerations:

Fourth Amendment considerations are central to the legal discourse surrounding multidisplay surveillance systems, particularly in relation to governmental use of these technologies. The Fourth Amendment of the United States Constitution protects against unreasonable searches and seizures, requiring that warrants be issued based on probable cause and describing the specific places to be searched and the items to be seized. However, the application of Fourth Amendment principles to emerging surveillance technologies poses complex challenges, as courts must grapple with defining what constitutes a "search" in the digital age and how traditional privacy expectations apply in public spaces subject to pervasive surveillance.

Courts have begun to address Fourth Amendment considerations in cases involving multidisplay surveillance systems, weighing the government's interest in public safety against individuals' privacy rights. For example, in the case of United States v. Jones (2012), the U.S. Supreme Court ruled that prolonged GPS monitoring of a suspect's vehicle constituted a search under the Fourth Amendment, highlighting the need for judicial scrutiny of government surveillance activities. Similarly, in Carpenter v. United States (2018), the Supreme Court held that the warrantless acquisition of historical cell phone location data violated the Fourth Amendment, signaling a recognition of the need for constitutional protections in the digital age.

The proliferation of multidisplay surveillance systems in public spaces raises questions about the reasonable expectation of privacy in areas subject to constant monitoring. While individuals may have diminished privacy expectations in public settings, the indiscriminate and pervasive nature of surveillance technologies challenges traditional notions of privacy and personal autonomy. Courts must grapple with balancing the government's legitimate interest in public safety with the individual's right to be free from unwarranted intrusion into their private affairs, particularly in spaces where individuals may have a reasonable expectation of anonymity and freedom from surveillance.

The use of multidisplay surveillance systems by law enforcement agencies raises concerns about the potential for abuse and misuse of surveillance powers. Without adequate safeguards and oversight mechanisms, there is a risk that these technologies could be deployed in a manner that disproportionately targets marginalized communities or infringes upon individuals' constitutional

rights. As such, courts play a critical role in ensuring that government surveillance activities comply with Fourth Amendment principles, holding law enforcement accountable for adhering to constitutional standards and safeguarding individuals' rights against arbitrary intrusion.

Fourth Amendment considerations are fundamental to the legal analysis of multidisplay surveillance systems, shaping the parameters of government surveillance and individuals' privacy rights. By applying constitutional principles to emerging surveillance technologies, courts play a vital role in upholding the balance between security interests and individual liberties, ensuring that surveillance activities are conducted within the bounds of the law and respect for constitutional rights.

Data Retention and Access:

Data retention and access policies are critical components of the legal framework governing multidisplay surveillance systems, dictating how long data collected by these systems is stored and who has access to it. The vast amount of data generated by multidisplay surveillance poses challenges regarding storage capacity, data security, and privacy protection. As such, regulations and guidelines must be established to ensure that data retention periods are proportionate to the legitimate purposes of surveillance and that access to stored data is restricted to authorized personnel for lawful investigative or security purposes.

One of the key considerations in data retention policies is striking a balance between the need for retaining data for investigative or evidentiary purposes and the imperative to minimize the risk of unauthorized access or misuse. Longer retention periods may enhance law enforcement capabilities by preserving potentially relevant evidence, but they also increase the risk of privacy breaches and data security vulnerabilities. As such, policymakers must carefully weigh the benefits and risks of prolonged data retention, taking into account factors such as the nature of the surveillance activity, the sensitivity of the data collected, and the potential impact on individuals' privacy rights.

Access to data collected by multidisplay surveillance systems must be strictly controlled to prevent abuse and ensure compliance with legal and procedural safeguards. Law enforcement agencies and other authorized entities may require access to surveillance data for legitimate investigative purposes, but such access should be subject to stringent oversight mechanisms, including judicial review and audit trails. Moreover, individuals whose data is captured by surveillance systems have a right to know how their information is being used and to request access to their own data, subject to appropriate safeguards to protect sensitive information and third-party rights.

Data retention and access policies must be designed to comply with applicable privacy laws and regulations, which may impose requirements regarding consent, transparency, and data minimization. For instance, the GDPR in the European Union mandates that personal data be processed lawfully, fairly, and transparently, with limited retention periods and strict limitations on access to sensitive data. Similarly, the CCPA in the United States grants consumers the right

to request access to and deletion of their personal information collected by businesses, including data captured by surveillance systems.

Data retention and access policies play a crucial role in shaping the legal landscape of multidisplay surveillance systems, balancing the need for retaining data for legitimate purposes with the imperative to protect individuals' privacy rights. By establishing clear guidelines for data retention periods, access controls, and transparency requirements, policymakers can ensure that surveillance activities are conducted in a manner that respects the rule of law and safeguards fundamental rights and freedoms.

Ethical Considerations in Multidisplay Surveillance:

Ethical considerations surrounding multidisplay surveillance systems are paramount, as these technologies have the potential to significantly impact individuals' rights, freedoms, and autonomy. One of the central ethical dilemmas posed by multidisplay surveillance is the tension between collective security interests and individual privacy rights. While surveillance systems may enhance public safety by deterring criminal activity and facilitating law enforcement efforts, they also have the potential to erode individuals' rights to privacy and autonomy, leading to a chilling effect on freedom of expression and association.

Transparency and accountability are also key ethical considerations in the deployment of multidisplay surveillance systems. The opacity surrounding surveillance practices and the lack of accountability mechanisms can undermine public trust in governmental and corporate entities responsible for overseeing these technologies. To mitigate these concerns, policymakers must prioritize transparency in surveillance operations, providing clear information about the scope, purpose, and impact of surveillance activities, as well as mechanisms for independent oversight and accountability.

Multidisplay surveillance systems raise ethical questions regarding the potential for discriminatory practices and bias in surveillance operations. The collection and analysis of vast amounts of data may exacerbate existing disparities and biases in law enforcement practices, leading to disproportionate surveillance and targeting of marginalized communities. Ethical frameworks must address these concerns by ensuring that surveillance activities are conducted in a manner that is fair, equitable, and nondiscriminatory, with safeguards in place to prevent the unjust targeting of certain groups or individuals based on factors such as race, ethnicity, or socioeconomic status.

Multidisplay surveillance systems present challenges to individual autonomy and freedom of movement, particularly in public spaces subject to constant monitoring. The pervasive nature of surveillance technologies can create a sense of surveillance creep, where individuals feel as though they are constantly being watched and scrutinized, leading to self-censorship and self-regulation of behavior. Ethical considerations dictate that individuals should have the right to move freely and engage in activities without fear of unwarranted surveillance, necessitating limitations on the scope and scale of surveillance activities to preserve individuals' autonomy and dignity.

Ethical considerations in multidisplay surveillance encompass a range of complex issues, including privacy, transparency, accountability, discrimination, and individual autonomy. By addressing these ethical concerns through robust ethical frameworks, policymakers can ensure that surveillance activities are conducted in a manner that respects individuals' rights and freedoms while promoting collective security and public safety in an increasingly surveilled world.

Individual Rights vs. Collective Security:

The tension between individual rights and collective security lies at the heart of ethical considerations surrounding multidisplay surveillance systems. On one hand, individuals have a fundamental right to privacy, autonomy, and freedom from unwarranted intrusion into their personal lives. Surveillance systems that encroach upon these rights risk undermining the very foundations of democratic societies, eroding trust between citizens and government entities, and chilling freedom of expression and association. Upholding individual rights is essential for safeguarding human dignity and preserving the rule of law in democratic societies.

On the other hand, collective security imperatives compel governments and organizations to deploy surveillance technologies to prevent and respond to threats to public safety. Multidisplay surveillance systems offer valuable tools for monitoring public spaces, detecting suspicious activities, and deterring criminal behavior. By enhancing situational awareness and enabling rapid response to security incidents, these systems contribute to the protection of communities and the maintenance of social order. However, the expansion of surveillance capabilities must be balanced against the potential erosion of individual rights, with safeguards in place to ensure that surveillance activities are proportionate, targeted, and conducted in accordance with the rule of law.

Finding the appropriate balance between individual rights and collective security is a complex ethical challenge that requires careful consideration of competing interests and values. Policymakers must weigh the potential benefits of surveillance technologies in enhancing public safety against the risks of infringing upon individuals' privacy and civil liberties. Moreover, ethical frameworks must incorporate principles of necessity, proportionality, and accountability to guide the responsible use of surveillance systems and mitigate the potential for abuse or misuse.

Ethical considerations dictate that individuals should have a voice in decisions regarding the deployment and operation of surveillance systems that may impact their lives. Public consultation, transparency, and accountability mechanisms are essential for fostering trust and legitimacy in surveillance practices, ensuring that the interests and perspectives of affected communities are taken into account in decision-making processes. By empowering individuals to participate in discussions about the trade-offs between security and privacy, policymakers can promote ethical decision-making and democratic governance in the realm of surveillance.

Reconciling individual rights with collective security imperatives is a complex ethical challenge that requires careful deliberation and balancing of competing interests. Ethical frameworks for

multidisplay surveillance systems must prioritize respect for individual autonomy, privacy, and dignity while also recognizing the importance of protecting communities and maintaining social order. By upholding principles of transparency, accountability, and public participation, policymakers can navigate this tension and ensure that surveillance activities are conducted in a manner that respects human rights and promotes the common good.

Transparency and Accountability:

Transparency and accountability are foundational principles in the ethical deployment and operation of multidisplay surveillance systems. Transparency requires that governments, organizations, and other entities responsible for surveillance activities provide clear and accessible information about the scope, purpose, and impact of surveillance operations. This includes disclosing the types of data collected, the methods used for data processing and analysis, and the entities with access to surveillance data. By promoting transparency, stakeholders can foster trust, facilitate public understanding, and encourage informed participation in discussions about the benefits and risks of surveillance technologies.

Accountability mechanisms are essential for ensuring that surveillance activities are conducted responsibly and in accordance with legal and ethical standards. Accountability entails holding individuals and organizations responsible for their actions, with mechanisms in place to address violations of privacy rights, abuses of power, and other misconduct. This may involve establishing oversight bodies, such as independent review boards or parliamentary committees, tasked with monitoring surveillance practices, conducting audits, and investigating complaints of abuse or misuse. Accountability mechanisms serve as checks and balances on government power, promoting adherence to the rule of law and safeguarding individuals' rights against arbitrary intrusion.

Transparency and accountability are essential for promoting legitimacy and public trust in surveillance practices. When stakeholders have confidence that surveillance activities are conducted transparently and subject to effective oversight, they are more likely to perceive these activities as legitimate and justifiable. Conversely, a lack of transparency and accountability can erode trust, fuel skepticism, and undermine public support for surveillance initiatives. By prioritizing transparency and accountability, governments and organizations can enhance the legitimacy of surveillance activities and promote public confidence in their effectiveness and fairness.

Transparency and accountability are integral to promoting democratic governance and protecting civil liberties in the realm of surveillance. In democratic societies, citizens have a right to know how their governments are using surveillance technologies and to hold decision-makers accountable for their actions. By promoting transparency in surveillance practices and ensuring robust accountability mechanisms, policymakers can uphold democratic principles, protect individuals' rights, and mitigate the risks of abuse and misuse of surveillance powers.

Transparency and accountability are essential ethical principles that must guide the responsible use of multidisplay surveillance systems. By promoting transparency in surveillance practices

and establishing effective accountability mechanisms, stakeholders can foster trust, promote legitimacy, and uphold democratic governance in the realm of surveillance. By prioritizing these principles, policymakers can strike a balance between security imperatives and individual rights, ensuring that surveillance activities are conducted in a manner that respects human dignity, privacy, and the rule of law.

Discriminatory Practices and Bias:

Discriminatory practices and bias represent significant ethical challenges in the context of multidisplay surveillance systems. These technologies have the potential to exacerbate existing inequalities and biases in law enforcement practices, leading to disproportionate surveillance and targeting of marginalized communities. For example, studies have shown that facial recognition algorithms used in surveillance systems often exhibit higher error rates when identifying individuals with darker skin tones, leading to increased risks of misidentification and wrongful targeting of minority groups. Such biases can perpetuate systemic discrimination and undermine trust in law enforcement among affected communities.

The deployment of multidisplay surveillance systems in public spaces may disproportionately impact certain demographic groups, such as racial minorities, low-income communities, and individuals with disabilities. Communities already subject to over-policing and surveillance may bear the brunt of intrusive surveillance practices, leading to feelings of stigmatization, alienation, and distrust towards authorities. Furthermore, discriminatory practices in surveillance operations can perpetuate social inequalities, exacerbating disparities in access to justice, employment, education, and other opportunities.

Addressing discriminatory practices and biases in multidisplay surveillance requires a multifaceted approach that encompasses technological, legal, and ethical interventions. Technological solutions, such as bias mitigation algorithms and fairness-aware machine learning techniques, can help minimize biases in surveillance systems and enhance the accuracy and fairness of algorithmic decision-making processes. However, technological solutions alone are insufficient to address the root causes of discrimination, which often stem from systemic inequalities, biases, and prejudices embedded within societal structures.

Legal and regulatory frameworks play a crucial role in combating discriminatory practices and bias in multidisplay surveillance. Anti-discrimination laws, such as the Civil Rights Act of 1964 in the United States and the Equality Act in the United Kingdom, prohibit discrimination on the basis of race, ethnicity, gender, religion, disability, and other protected characteristics. These laws provide avenues for individuals and communities affected by discriminatory surveillance practices to seek redress and hold accountable entities responsible for perpetuating bias and discrimination.

Ethical considerations dictate that surveillance practices should be conducted in a manner that is fair, equitable, and nondiscriminatory, with safeguards in place to prevent the unjust targeting of certain groups or individuals. Ethical guidelines for surveillance operations should prioritize principles of fairness, transparency, accountability, and respect for human rights, ensuring that

surveillance technologies are deployed in a manner that upholds the dignity and rights of all individuals, regardless of their race, ethnicity, religion, gender, or socioeconomic status. By addressing discriminatory practices and biases in multidisplay surveillance, stakeholders can promote social justice, equity, and inclusion in the design and implementation of surveillance systems.

Case Studies: Real-world Applications and Impacts:

Case studies provide valuable insights into the real-world applications and impacts of multidisplay surveillance systems across various sectors and contexts. For instance, in the realm of law enforcement and public safety, cities like London and New York have implemented extensive surveillance networks comprising CCTV cameras, facial recognition technology, and other surveillance tools to monitor public spaces and detect criminal activity. These systems have been credited with assisting law enforcement agencies in apprehending suspects, preventing crimes, and enhancing overall security. However, they have also raised concerns about privacy infringement, civil liberties violations, and the potential for discriminatory targeting, prompting debates about the ethical and legal implications of pervasive surveillance.

In the workplace, employers are increasingly deploying multidisplay surveillance systems to monitor employees' activities, productivity, and behavior. For example, retail stores may use surveillance cameras equipped with facial recognition technology to track customer demographics and preferences, while office environments may implement keystroke logging software to monitor employees' computer usage and productivity levels. While proponents argue that such surveillance measures improve efficiency, security, and accountability, critics raise concerns about employee privacy, autonomy, and dignity, highlighting the need for clear guidelines and safeguards to protect workers' rights in the digital workplace.

Smart city initiatives and urban monitoring programs represent another area where multidisplay surveillance systems are being deployed to collect data on urban environments and population dynamics. For example, cities like Singapore and Barcelona have implemented smart city technologies, including sensors, cameras, and data analytics platforms, to monitor traffic flow, manage public utilities, and enhance urban planning efforts. While these initiatives promise to improve efficiency, sustainability, and quality of life, they also raise concerns about data privacy, surveillance creep, and the potential for authoritarian governance, underscoring the importance of ethical oversight and citizen engagement in shaping the future of urban surveillance.

Multidisplay surveillance systems have been used in the context of border security and immigration enforcement to monitor and control the movement of people across national borders. For instance, countries like the United States and European Union have implemented surveillance technologies, including drones, biometric scanners, and automated facial recognition systems, to monitor border crossings, detect unauthorized migrants, and enforce immigration laws. These systems have sparked debates about human rights, refugee protection, and the militarization of borders, highlighting the need for ethical considerations and humanitarian safeguards in border surveillance practices.

Case studies of real-world applications and impacts of multidisplay surveillance systems illustrate the complexities and challenges inherent in deploying these technologies in diverse contexts. While surveillance systems offer potential benefits in terms of security, efficiency, and public safety, they also raise significant ethical, legal, and social concerns that must be addressed through transparent governance, accountability mechanisms, and respect for human rights and civil liberties. By examining case studies and lessons learned from various sectors, stakeholders can better understand the implications of surveillance technologies and develop policies and practices that uphold democratic values and promote the common good.

Summary:

The legal and ethical landscape surrounding multidisplay surveillance systems is intricate and multifaceted, intersecting with issues of privacy, civil liberties, and the balance between security and individual freedoms. By examining these implications through the lenses of existing laws, ethical principles, and real-world case studies, this paper sheds light on the complexities inherent in regulating and governing such surveillance technologies. Moving forward, thoughtful consideration and robust regulatory frameworks are essential to navigate the evolving landscape of surveillance in an increasingly interconnected world.

References:

- Solove, D. J. (2006). Understanding Privacy. Harvard University Press.
- Westin, A. F. (1967). Privacy and Freedom. Atheneum.
- Rosen, J. (2019). The Unwanted Gaze: The Destruction of Privacy in America. Vintage.
- Rothstein, M. A. (2010). Genetic Secrets: Protecting Privacy and Confidentiality in the Genetic Era. Yale University Press.
- Electronic Frontier Foundation. (n.d.). Surveillance Self-Defense. Retrieved from https://ssd.eff.org/
- Solove, D. J. (2008). Understanding Privacy. Harvard Law Review, 127(7), 1965-2059.
- Lessig, L. (2006). Code: And Other Laws of Cyberspace. Basic Books.
- Nissenbaum, H. (2009). Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press.
- Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. Harvard Law Review, 4(5), 193-220.
- Rule, J. B. (1973). Private Lives and Public Surveillance: Social Control in the Computer Age. Schocken Books.
- Garfinkel, S. L. (2000). Database Nation: The Death of Privacy in the 21st Century. O'Reilly Media, Inc.
- Allen, A. L. (2004). Privacy Law and Society. West Academic.
- Federal Trade Commission. (n.d.). Privacy & Data Security. Retrieved from https://www.ftc.gov/tips-advice/business-center/privacy-and-security
- Koops, B.-J., Newell, B. C., Timan, T., & Skorupskaite, E. (2018). A Typology of Privacy. University of Pennsylvania Journal of International Law, 38(2), 483-575.
- Bygrave, L. A. (2002). Data Protection Law: Approaching Its Rationale, Logic and Limits. Kluwer Law International.
- Gellman, R. (2017). Privacy's Double Standard. The Harvard Law Review Forum, 127, 35-48.
- Regan, P. M. (1995). Legislating Privacy: Technology, Social Values, and Public Policy. The University of North Carolina Press.
- Clarke, R. (1988). Information Technology and Dataveillance. Communications of the ACM, 31(5), 498-512.
- Rotenberg, M., & Fuentes, C. (2000). Privacy and Human Rights Report. Electronic Privacy Information Center (EPIC).
- Tene, O., & Polonetsky, J. (2013). Big Data for All: Privacy and User Control in the Age of Analytics. Northwestern Journal of Technology and Intellectual Property, 11(5), 239-273.
- Hildebrandt, M. (2008). Defining Profiling: A New Type of Knowledge? In B. Schneier (Ed.), Security and Privacy: Silver Linings in the Cloud (pp. 35-52). Wiley Publishing.
- Pasquale, F. (2015). The Black Box Society: The Secret Algorithms That Control Money and Information. Harvard University Press.