Heidi Mork Lomell

44 Privatization

Abstract: Almost every aspect of the digital is private. To understand digitization, we therefore need to understand privatization. This chapter outlines some of the aspects of privatization by exploring major differences between a public and a private approach to criminalization, crime, and control.

Keywords: privatization, private space, regulation, commercial logics

Introduction

On January 6, 2021, a mob of Donald Trump's supporters attacked Capitol Hill in an attempt to prevent the US Congress from approving the victory of president-elect Joe Biden. After the attacks, Facebook, Instagram, Twitter, Snapchat, and YouTube suspended Donald Trump's accounts because of the role his social media posts played in inciting the violence and also due to the risk of inciting further attacks (Mamak, 2023). This was not a result of a police investigation, a criminal charge, or a court verdict. Suspension from social media is not a punishment for a crime committed, but a result of a decision made by the social media companies for breaking their terms of services. To some, the suspensions demonstrated that no one is above the law. For others, the case illustrates that we all are, just as Donald Trump was, subject to the arbitrary and unaccountable power of companies (Floridi, 2021).

Much of our personal, social, and professional life has migrated onto private platforms (see Platforms by Egbert). Both private citizens and public institutions are increasingly dependent on a privatized, digital infrastructure (Andrejevic, 2013). Almost every aspect of the digital is private: private companies invent, design, produce, sell, maintain, and in many respects even *govern* the digital (Floridi, 2020).

This raises several questions for criminologists. Criminalization, crime, and crime control have traditionally been understood and studied as public issues. These are fields inhabited by public and political actors such as lawmakers, bureaucrats, police officers, judges, and prison guards. What happens when private and commercial interests enter these fields through digitization? How do we approach the role of private interests in digital criminology?

The private foundation of digital technologies is a key component for studying crime and crime control in digitized societies. To understand digitization, we need to

Disclaimer and acknowledgments: The chapter is written as part of the CRIMKNOW project (Private knowledge, public issues: Digitalization and private economies of knowledge in criminal justice), financed by the Research Council of Norway (project no. 334953).

understand privatization, especially some of the major differences between a public and a private approach to our core topics: criminalization, crime, and control.

In this entry, I will explore how the concept of privatization offers an important point of departure for understanding digital criminology. I will start by taking a closer look at the concept itself and its counterpart: the private and the public. I will then explore what is meant by privatization and how privatization has been studied in criminology, before addressing some of the major issues in digital criminology through the lens of privatization.

Private and public

The categories of public and private are central in structuring our social lives (d'Entrèves and Vogel, 2000: 1). 'Public' is associated with the state, with politics, and with the community, while 'private' is associated with the economy, the market, but also the home, the family, and the personal. We use these categories to distinguish between sectors, such as the state and the economy, the political and the market, and the government and the private citizen. We also use them to distinguish between realms or spaces, either literally, for instance land or property, or more figuratively, for instance information or data. A public space is in principle accessible and open for all, while private space has limited access. In some countries, information such as your annual income or your criminal record is considered public, while in other countries this information is considered private. Some data are public, such as the crime statistics, which is produced by the police and the courts, while other data are private, for example data from social media platforms on search patterns.

What is private and what is public varies in time and space. And even if we can view the concepts as binaries, there are and have always been overlaps. For example, private markets are not entirely free from public regulation, and the private home is not totally secluded from public interventions—whether it is regulations and inspections concerning electricity and fire protection, or the child protection services inspecting a home due to a report of concern.

Even before digitization, the demarcation between public and private was blurry. With digitization, such distinctions have become even more complex. Private data or information can easily be made public, either by consent or against a person's will. One example is how we increasingly both document and share our private life online, and thereby to broader publics than before.

Some private social media platforms are defined as a public space by law. Our 'private' messages or posts on social media platforms can therefore be defined and treated by law as 'public'; offensive comments made on private social media accounts have led to prison sentences (Rustin, 2014). Even on platforms that require a login to access, private information, communication, and images risk becoming public through 'sharing' functions (Powell et al., 2018: 28). In 2018, more than 1,000 young people in Denmark were charged for the possession and sharing of child pornography, indecency, and wrongfully disclosing of private affairs after sharing two video sequences containing sexual material involving persons under the age of 18 on the Facebook chat-platform Messenger (Holst and Adolphsen, 2020). These examples illustrate that our understanding of what is defined as private and public online is still developing.

Another complicating factor is that these platforms are developed, owned, administrated, and regulated by private corporations. This means that even if we choose to be or are defined by law as ‘public’ in our online life, we are literally on private grounds and subject to their norms and regulations.

Privatization

Privatization means that public goods, services, and/or space are overtaken by private companies. During the 1990s a range of network utilities, from telecommunications, power supplies to railways, were privatized in many countries (Offer, 2022). In its purest form privatization implies the total transfer of public assets to the private sector as manifested in the selling off of state-owned businesses, industries, and utilities (Hamerton and Hobbs, 2022: 4). However, the concept is used to refer to a wide range of processes, from the sale or contracting out of public institutions to private companies, to various forms of deregulation (Matthews, 1989: 1).

In some cases, privatization implies transferring industries and/or services *back* to the private sector: The growth of the social welfare state implied the public taking over the responsibility of the welfare of the people. In other words, what preceded the privatization of the public sector was a ‘publicization’ of private services with the rise of, for example, public social security, public health services, public transport, public schools, etc. Even policing functions were ‘private’ before the establishment of the modern, public police (Zedner, 2006). Crime was a branch of torts, where the victim had to bear the costs of law enforcement and prosecution, and compensation dominated over retribution (Feeley, 2018).

Privatization in criminology and criminal justice

While privatization was the buzzword of the 1980s and 1990s, proposals to privatize parts of the criminal justice system were met with “a widespread sense of bemused disbelief” as it was widely assumed that “the provision of laws, punishment and crime control constitute a unique and privileged realm of activity that should be provided by the State” (Matthews, 1989: 1). The monopoly over the use of legitimate force is one of the essential characteristics of a state. Nevertheless, Matthews and colleagues documented that there already existed a significant degree of privatization within the criminal justice system.

Since the 1980s, criminologists gained considerable insight into the emergence and impact of new configurations of the state and the private sector in certain areas of crime and security governance—often framed as the rise of neo-liberal forms of governance (Crawford, 2006). In his seminal work *Crime Control as Industry* in 1993, Christie documented how the growth in prison sentences in the US was closely related to the privatization of prisons (Christie, 2000). Within policing and security studies, Clifford Shearing and Philip Stenning published several studies in the 1980s and set the ground for a flourishing research tradition on both private security providers and the privatization of public policing (Johnston, 1992; Jones and Newburn, 1998; Shearing and Stenning, 1981, 1985, 1987; Wakefield, 2003). The increasing privatization of crime control and security continue to draw attention within criminology and criminal justice studies, however, often neglecting the digital aspects of the development (Daems and Beken, 2018; Hamerton and Hobbs, 2022; Hucklesby and Lister, 2018; Simmons, 2023).

The growth in private policing and private security has been connected to the parallel growth in 'mass private property,' which is privately owned land that is open or partly open to the public, often policed by private regulation and private security services. Examples include shopping malls, airports, amusement parks, and gated communities. The rules and regulations that govern such places are not primarily the criminal law, but rather (or in addition), corporate house rules and property law. Research has shown that these privately owned, semi-public or public places are policed not for the enforcement of criminal law, but rather for the purposes of both restricting public access and maximizing profit (Shearing and Stenning, 1981, 1985). Private security companies do not uphold public order and the rule of law, but the private order of their clients (Shearing, 1992).

Criminological research on the consequences of privatization has strong links to surveillance studies (Lyon, 2007). Both fields have studied the implications of privatization on issues on both social and crime control and more specifically on surveillance practices (see Surveillance by Lyon). The findings implicate that privatized public space is controlled by other norms, with other means and with other consequences than public space controlled by public police (Lomell, 2004). Private control is based on an instrumental, not moral, foundation, where order is whatever maximizes profit. The instrumental language of profit and loss replaces the moral language of criminal justice. Control becomes consensual, and rule-breaking leads to exclusion and banishment (Shearing and Stenning, 1985).

Corporate and state surveillance merge and promise both increased security from the state and increased convenience from the corporations (Giroux in Powell et al., 2018: 55). These differences between corporate and state surveillance resembles earlier studies of the logic of private control. Shearing and Stenning pointed to the instrumental and commercial underpinnings of privatized control instead of the moral basis of criminal justice (Shearing and Stenning, 1985). Also, Zygmunt Bauman has highlighted the more seductive dimensions of private surveillance and control: "everything moves from enforcement to temptation and seduction; surveillance society no longer chases its victims but finds its volunteers" (in Walker-Munro, 2023: 121).

Privatization and digital criminology

The findings from criminological research on privatization are a valuable starting point for researching privatization in digitized societies. Important questions to ask are: Who makes the rules, what are they, who are the control agents, what are their powers, and what are the consequences of rule-breaking?

For digital criminology, privatization means something different than privatizing institutions and practices that were previously run by public service. In digitized societies, many private, social, public, and professional aspects of life are interlinked with privately run social media platforms and computer programs. This is new. The private sector has always been part of society, but now it is increasingly providing the digital infrastructure for both citizens and governments (see Infrastructures by Grisot and Parmiggiani). We rely upon the private sector for the provision of digital utilities and services such as communication, search engines, programs, and storage. This deserves attention. Not only is it relevant to study the consequences of building a digital society on the premises of private companies, both literarily and symbolically. Criminologists should further ask how this trend affects law-making, law-breaking, and law enforcement. Here, the commercial logics that permeate digital technologies are key. While many of us think of digital space as public—or at least semi-public, the owners remain private. The 'digital commons' are private commons where we are first and foremost consumers and products, and only secondly citizens with rights.

Most, not all, digital infrastructures have been private and commercial from the outset. Despite this, the concept privatization is useful, because it helps us to focus on how our daily life in our digital societies and on digital platforms are more and more taking place on platforms and programs governed by corporate law and regulations. This has profound consequences for crime and crime control.

One example is the growth and impact of the companies' 'terms of services' that take on the role of criminal law and procedure for the regulation of online behavior, as we saw with the suspension of Donald Trump's social media accounts. Traditionally, criminologists use criminal law and criminal justice agencies as their point of departure for studying behavior. The process of law-making, law-breaking, and law enforcement requires a law. Online, however, concepts such as 'community standards' and 'terms of services' have gained prevalence. The process of making, breaking, and enforcing them are less transparent for users but also for researchers alike. And yet, they can have severe impact for the individual. On Facebook,[1] for example, users may report posts and comments as 'inappropriate' or 'controversial.' The result of reporting might be a 'Facebook jail sentence,' [2] which means being denied posting for a certain amount of time. Such a 'sentence' is imposed by automated or real 'Facebook

[1] https://transparency.meta.com/policies/community-standards/

[2] https://www.online-tech-tips.com/facebook-jail-how-you-will-be-punished-for-misbehaving-on-facebook/

censors,' and might have severe consequences for people, either professionally or personally (McGoldrick, 2013). While banishment is an old form of punishment and widely used by private security companies (Lomell, 2004), 'cyber-banishment' (Mamak, 2023), or 'withdrawal of system access authorization' (R. Jones, 2000), represents the digital version, currently enforced by the platforms' private owners.

The fact that digitized public space is private at its base, then, shapes and controls the norms and behaviors of its users. One key aspect is here that companies are first and foremost focused on profit, not justice, nor democracy: "While privately-owned social media platforms are nominally facilitating democratic engagement, they are primarily optimized for data retention, advertising exposure and other profit-making strategies" (Powell et al., 2018: 54). Zuboff famously coined the term *surveillance capitalism* to describe the current situation where online data is extracted and monetized; often without consent (Zuboff, 2019).

Privatization of knowledge production

The data that users produce online are a central component of corporations' business models (Walker-Munro, 2023). They provide companies with valuable insights into their consumers. Corporations therefore routinely collect more data than strictly necessary. One example is the company TikTok that captures the location, calendar, and contacts of its users, in addition to all other apps installed on the phone. While this information appears to serve no valid purpose for delivering TikTok's services (Perkins in Walker-Munro, 2023: 122), it is valuable, as these data can be of interest to other corporations and to national or foreign security services. Another example is Cambridge Analytica, who used a Facebook quiz to collect personal information of around 87 million users and then used that information to generate political and voter insights that was then sold on to political campaigns and parties (Brayne, 2020: 24).

Private companies collect and aggregate information from both private sources and public records to make these data available to those who can pay the fee for access. The police does not only buy data collected by private companies; they also use private sector platforms to store, share, and analyze data they themselves have collected (Brayne, 2020: 25). So-called predictive policing is based on software, systems, and algorithms developed by companies such as PredPol, HunchLab, IBM and Palantir (Brayne, 2020; see Policing by Wilson).

One important but overlooked aspect of privatization in digital criminology is the privatization of knowledge production. The knowledge base of contemporary criminal justice is, due to extensive digitization and marketization, undergoing fundamental transformations that involve a greater prominence of private actors and their logics. Private and hybrid knowledge providers, such as consultancies and NGOs, depart from established traditions for transparency as well as scientific and democratic oversight in criminology and criminal justice. The role of private actors in contemporary criminal justice policy development and implementation is a topic that deserves attention from digital criminologists since they are intrinsically linked to the development and sale of digital infrastructures.

Conclusion

Criminology's core topics are first and foremost public issues. Digital criminology, with its focus on how digitization alters criminalization, crime, and crime control, will benefit from paying attention to the private actors and logics that are fundamental to digitization: "it is ultimately the private companies who regulate these spaces, determining who has access, which content is to be shared, how widely it is viewed [...] and on what grounds it is removed. In this corporatisation of both public and private life, companies such as Facebook and Google engage in practices of 'networked authoritarianism' and 'corporate censorship'" (Powell et al., 2018: 28).

It is therefore important to turn our attention to the publicness/privateness of various actors in criminal justice, but also in the privatized governance of the digital realm. A crucial task is to study similarities and differences in modes of thinking about regulation and control between public and private actors within the field of digital criminology. If the governance of the digital realm is left to private enterprises, business strategies, self-regulation and market forces, long-held criminal justice principles such as the rule of law, due process, proportionality, and a right to a fair trial, not to mention democratic oversight, accountability and transparency, risk being disregarded in increasingly crucial areas of contemporary societies (Floridi, 2021).

Main takeaways

- Almost every aspect of the digital is private: private companies invent, design, produce, sell, maintain, and in many respects even *govern* the digital.
- To understand digitization, we need to understand privatization, especially some of the major differences between a public and a private approach to our core topics: criminalization, crime, and control.
- Important questions to ask when studying digital platforms are: What data do platform owners have access to? Who makes the rules, what are they? Who are the control agents, what are their powers and what are the consequences of rule-breaking?

Suggested reading

Brayne, S. (2020). *Predict and Surveil: Data, Discretion, and the Future of Policing.* New York: Oxford University Press, USA.

Hamerton, C., & Hobbs, S. (2022). *Privatising Criminal Justice: History, Neoliberal Penality and the Commodification of Crime.* London: Routledge.

Simmons, R. (2023). *Private Criminal Justice: How Private Parties Are Enforcing Criminal Law and Transforming Our Justice System.* Cambridge: Cambridge University Press.

References

Andrejevic, M. (2013). Exploitation in the data mine. In C. Fuchs, K. Boersma, A. Albrechtslund, & M. Sandoval (eds.), *Internet and Surveillance: The Challenges of Web 2.0 and Social Media* (pp. 71 – 88). New York: Routledge.

Brayne, S. (2020). *Predict and Surveil: Data, Discretion, and the Future of Policing.* Oxford: Oxford University Press, USA.

Christie, N. (2000). *Crime Control as Industry. Towards Gulags, Western Style.* London: Routledge.

Crawford, A. (2006). Networked governance and the post-regulatory state? *Theoretical Criminology*, 10(3), 449 – 479.

d'Entrèves, M. P., & Vogel, U. (2000). Public and private: A complex relation. In M. P. d'Entrèves & U. Vogel (eds.), *Public and Private. Legal, Political and Philosophical Perspectives* (pp. 1 – 16). London: Routledge.

Daems, T., & Beken, T. V. (2018). *Privatising Punishment in Europe?* London: Routledge.

Feeley, M. M. (2018). Privatizing criminal justice: A historical analysis of entrepeneurship and innovation. In T. Daems & T. V. Beken (eds.), *Privatising Punishment in Europe?* (pp. 26 – 52). New York: Routledge.

Floridi, L. (2020). The fight for digital sovereignty: What it is, and why it matters, especially for the EU. *Philosophy & Technology*, 33(3), 369 – 378.

Floridi, L. (2021). Trump, Parler, and regulating the infosphere as our commons. *Philosophy & Technology*, 34(1), 1 – 5.

Hamerton, C., & Hobbs, S. (2022). *Privatising Criminal Justice: History, Neoliberal Penality and the Commodification of Crime.* London: Routledge.

Holst, N. S., & Adolphsen, C. (2020). Adolescents and sexual violations online. *Juvenile and Family Court Journal*, 71(3), 43 – 55.

Hucklesby, A., & Lister, S. (eds.) (2018). *The Private Sector and Criminal Justice.* London: Palgrave Macmillan.

Johnston, L. (1992). *The Rebirth of Private Policing.* London: Routledge.

Jones, R. (2000). Digital rule. Punishment, control and technology. *Punishment & Society*, 2(1), 5 – 22.

Jones, T., & Newburn, T. (1998). *Private Security and Public Policing.* Oxford: Clarendon Press.

Lomell, H. M. (2004). Targeting the unwanted. Video surveillance and categorical exclusion in Oslo, Norway. *Surveillance & Society*, 2(2/3), 346 – 360.

Lyon, D. (2007). *Surveillance Studies. An overview.* Cambridge: Polity Press.

Mamak, K. (2023). Cyber banishment: An old sanction for virtual spaces. *Criminal Justice Studies*, 36(2), 133 – 145.

Matthews, R. (ed.) (1989). *Privatizing Criminal Justice.* London: Sage Publications.

McGoldrick, D. (2013). The limits of freedom of expression on Facebook and social networking sites: A UK perspective. *Human Rights Law Review*, 13(1), 125 – 151.

Offer, A. (2022). *Understanding the Private–Public Divide: Markets, Governments, and Time Horizons.* Cambridge: Cambridge University Press.

Powell, A., Stratton, G., & Cameron, R. (2018). *Digital Criminology: Crime and Justice in Digital Society.* New York: Taylor and Francis.

Rustin, S. (2014, June 13). Is it right to jail someone for being offensive on Facebook or Twitter? *The Guardian.* https://www.theguardian.com/law/2014/jun/13/jail-someone-for-being-offensive-twitter-facebook

Shearing, C. D. (1992). The relation between public and private policing. In M. Tonry & N. Morris (eds.), *Modern Policing* (Vol. 15) (pp. 399 – 434). Chicago: The University of Chicago Press.

Shearing, C. D., & Stenning, P. C. (1981). Modern private security: Its growth and implications. In M. Tonry & N. Morris (eds.), *Crime and Justice: An Annual Review of Research* (Vol. 3) (pp. 193 – 245). Chicago: Chicago University Press.

Shearing, C. D., & Stenning, P. C. (1985). From the panopticon to Disney World: The development of discipline. In A. N. Doob & E. L. Greenspan (eds.), *Perspectives in Criminal Law* (pp. 335 – 349). Toronto: Canada Law Book Inc.

Shearing, C. D., & Stenning, P. C. (1987). *Private Policing* (Vol. 23). London: SAGE Publications.

Simmons, R. (2023). *Private Criminal Justice: How Private Parties Are Enforcing Criminal Law and Transforming Our Justice System.* Cambridge: Cambridge University Press.

Wakefield, A. (2003). *Selling Security. The Private Policing of Public Space.* Cullompton: Willan Publishing.

Walker-Munro, B. (2023). Hyper-collection: A possible new paradigm in modern surveillance. *Surveillance & Society*, 21(2), 120 – 138.

Zedner, L. (2006). Policing before and after the police. *British Journal of Criminology*, 46, 78 – 96.

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for the Future at the New Frontier of Power.* New York: Profile Books PublicAffairs.