QUEEN'S UNIVERSITY BELFAST

The punitive mesh: digital presence, mutual surveillance, and participatory punishment in networked societies

Corda, A. (2026). The punitive mesh: digital presence, mutual surveillance, and participatory punishment in networked societies. *Punishment and Society*. Advance online publication. https://doi.org/10.1177/14624745261437539

Published in:
Punishment and Society

Document Version:
Publisher's PDF, also known as Version of record

Queen's University Belfast - Research Portal:
Link to publication record in Queen's University Belfast Research Portal

Publisher rights
Copyright 2026 the authors.

This is an open access article published under a Creative Commons Attribution-NonCommercial License (https://creativecommons.org/licenses/by-nc/4.0/), which permits use, distribution and reproduction for non-commercial purposes, provided the author and source are cited.

General rights
Copyright for the publications made accessible via the Queen's University Belfast Research Portal is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

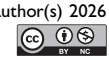
Take down policy
The Research Portal is Queen's institutional repository that provides access to Queen's research output. Every effort has been made to ensure that content in the Research Portal does not infringe any person's rights, or applicable UK laws. If you discover content in the Research Portal that you believe breaches copyright or violates any law, please contact openaccess@qub.ac.uk.

Open Access
This research has been made openly available by Queen's academics and its Open Research team. We would love to hear how access to this research benefits you. – Share your feedback with us: http://go.qub.ac.uk/oa-feedback

Download date:10. Nov. 2026

Check for updates

Normal manuscript

Punishment & Society
1–23
© The Author(s) 2026

Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/14624745261437539
journals.sagepub.com/home/pun


The punitive mesh: Digital presence, mutual surveillance, and participatory punishment in networked societies

Alessandro Corda[1]

Abstract

This article explores the emergence of a pervasive system of social control in contemporary networked societies, termed the "punitive mesh." Building on the dispersal of penal power and surveillance dynamics theorized by Foucault, Deleuze, Cohen, and Zuboff, the punitive mesh captures how punishment and reputational judgment extend beyond formal institutions, circulating laterally and diffusely through digital infrastructures. It encompasses persistent digital traces, public criminal records, informal review platforms, and viral social media content, where ordinary users both administer and experience sanctions. Within this landscape, the boundaries between the punisher and the punished, public and private, and formal and informal authority are blurred, and social participation itself becomes a mechanism of enforcement. The article examines how these dynamics enable participatory punishment, through which reputational harm is produced, amplified, and perpetuated via collective engagement rather than official sanctions. By analyzing the interplay of exposure, circulation, and persistence across online networks, the punitive mesh reveals how social control is continuous, decentralized, and mutually enforced. This framework highlights the challenges posed by networked sanctioning for justice, privacy, and social life, showing that punishment is no

[1]School of Law, Queen's University Belfast, Belfast, UK

Corresponding author:
Alessandro Corda, School of Law, Queen's University Belfast, Main Site Tower, University Square, Belfast, BT7 1NN, UK.
Email: A.Corda@qub.ac.uk

longer episodic or institutionally contained but embedded within the infrastructure of everyday digital interaction.

Keywords
punitive mesh, social control, participatory punishment, reputational harm, digital surveillance, privacy

Introduction

In 1979, Stanley Cohen articulated an emergent vision of penal power that challenged the institutional and spatial assumptions of traditional punishment. In his article *The punitive city: Notes on the dispersal of social control*, Cohen described a newly evolving penal world in which incarceration was no longer the sole—or even the central—form of punishment. Instead, penal power was dispersing outward, infiltrating community spaces, workplaces, and even private life. Cohen's metaphor of the punitive city captured a profound shift: the relocation of punishment from bounded, state-run institutions to a diffuse, socially embedded system. What he could not yet have foreseen, however, was the way in which this punitive geography would be further transformed—and, indeed, intensified—by the rise of digital technologies. In the decades since the publication of his influential paper, we have witnessed the emergence of a punitive ecosystem that extends far beyond the reach of state authority, and evolved into networked and participatory forms of surveillance and sanctioning that are both omnipresent and almost inescapable.

Consider, for instance, the evolving context of publicly accessible criminal records. Until a few decades ago, the legal principle of "open justice" was tempered by the practical frictions of access: to discover a criminal conviction, one often had to attend court hearings in person, request physical files, or navigate bureaucratic processes. The effort involved and the lack of mass dissemination imposed natural limits on the social consequences of a criminal record (Corda, 2016; Jacobs, 2015). Today, however, those frictions have been largely eradicated. Criminal records, court filings, and mugshots are, for the most part, instantly searchable on the internet, aggregated by commercial databases, and disseminated through news articles that remain online indefinitely. Even when charges are dropped or convictions expunged, the digital trace often persists, accessible to employers, landlords, neighbors, or casual acquaintances (Corda and Lageson, 2020; Lageson, 2020; Reosti et al., 2024: 538–539). The mere fact of having been accused can become a permanent feature of one's digital identity (Lageson and Kaplun, 2021).

Yet the contemporary punitive landscape is not confined to the online permanence of formal legal records. Increasingly, in today's digital age, reputational judgments are no longer restricted to information generated within or stemming from the slow machinery of the official criminal justice system (Strahilevitz, 2008). Instead, they are produced, amplified, and enforced through a vast ecosystem of informal, extra-legal platforms—

ranging from "whisper network" apps such as Tea (Hunter, 2025) and Facebook groups such as "Are We Dating the Same Guy?" (Al-Othman, 2025), allowing women to post reviews, backgrounds, and experiences of men they have dated or are interested in, to consumer review platforms such as Google Reviews (Payne, 2024) and niche rating forums such as RateMyProfessor (Nowicki, 2024). These spaces allow ordinary users to publicly evaluate, shame, or vindicate others with a few keystrokes, at a speed and scale the formal justice system cannot match. The result is a form of participatory punishment —swift, networked, and enduring—where the verdict is rendered in the court of public opinion and the sentence is embedded in online memory.

These developments reveal a paradox. On the one hand, contemporary societies are increasingly preoccupied with privacy. We worry about the reach of state surveillance, the tracking capacities of corporations, and the commodification of personal data (e.g., Brayne, 2022; Gilliom and Monahan, 2012; Haggerty and Ericson, 2000; Lyon, 2007; Marx, 2016; Nissenbaum, 2004; Taylor, 2002). Similarly, the rhetoric of privacy rights is a mainstay of public discourse, informing legislation such as the EU's General Data Protection Regulation (GDPR) (Bennett, 2018) and countless debates about "big tech" overreach (Birch and Bronson, 2022). On the other hand, ordinary individuals willingly participate in systems of information sharing and reputational control, often with unreserved enthusiasm or, at least, resigned awareness (Oguafor and Nevzat, 2023).[1] We review and rate strangers on Airbnb and Uber (Christiaens, 2025; Tadelis, 2016), report suspicious behavior on neighborhood watch apps (Kennedy and Coelho, 2022; Parker and Dodge, 2024), post screenshots of private conversations to social media (Ingber, 2025), and much more.[2] Privacy is championed as a value when we are the ones under scrutiny, yet the drive to scrutinize and expose others remains deeply entrenched, and at times openly celebrated (Gallagher et al., 2019).

This paradox cannot be reduced to hypocrisy. It reflects, instead, a profound transformation in the ecology of social control. Foucault (1995 [1975]) illuminated the shift from spectacular, centralized punishment to a regime of diffuse disciplinary power, exemplified by Bentham's Panopticon, whose mode and logic of surveillance become internalized and dispersed throughout society, a dynamic that Deleuze (1992) later situated within broader "societies of control." Cohen (1979), as mentioned, built upon this, exploring how penal power migrated into community life, dissolving the walls between prison and society. Zuboff (2019) reframed surveillance in the context of platform economies, where personal data are commodified and behavioral modification is driven by profit motives. These frameworks are key to understand the rise of mutual forms of "lateral surveillance" (Andrejevic, 2004, 2006) in which the boundaries between state, market, and citizens become so thoroughly entangled that they no longer operate as meaningfully distinct analytic categories.

The present-day landscape, I argue, is best conceptualized as a "punitive mesh." Unlike the institutional gaze of the Panopticon or the spatial dispersal of the punitive city, the mesh is a network with no single, discernible center. It is constituted by countless points of observation and judgment, linked by digital infrastructures that ensure the rapid circulation and indefinite retention of information. In the mesh, reputational harm can be inflicted as easily by a neighbor's Facebook or X/Twitter post as by a criminal court's judgment. The same

individual can be a subject of surveillance in one moment and its agent in the next. Furthermore—and crucially—the mesh is not merely a consequence of state policy or corporate strategy; it is also actively sustained through ordinary social participation.[3]

Under this framework, publicly accessible and commodified criminal records, informal reputational platforms, and viral video postings represent three strands of the same mesh. Each operates through a logic of exposure, disseminating information about past conduct—whether verified or merely alleged—in ways that reshape opportunities, relationships, and social standing, and, in some cases, incentivizing forms of real-life vigilante justice (Cubellis et al., 2018; Johnston, 1996; Reosti et al., 2024: 539–542) or digital vigilantism (Chia, 2020; Loveluck, 2019; Trottier, 2017). In all these cases, the harm extends beyond the initial moment of censure, sustained by the persistence and searchability of digital traces. Redemption, conceived as both personal transformation and meaningful reintegration into the community, becomes increasingly difficult when the past remains perpetually accessible and shareable (Ambrose et al., 2012; Lageson and Corda, 2024: 37–40; Lageson and Maruna, 2017; Murphy et al., 2011).

In today's networked societies, one does not enter or leave the punitive mesh; individuals are already and constantly within it. Its logic is not that of walls and gates but of nodes and links, of endless connection. And unlike traditional state punishment dispensed and administered by a centralized authority, the mesh distributes its authority in an omnidirectional way. Control and sanctions are imposed and enacted not only from the top down but also laterally, from citizen to citizen, user to user. The result is a form of punishment that is continuous, participatory, and unmoored from the procedural safeguards of the legal system.

After tracing its theoretical lineage, this article presents and develops the concept of the "punitive mesh" as a way of theorizing the convergence of disciplinary power, fluid mechanisms of control, dispersed punishment, and surveillance capitalism into a new integrated ecology of sanctioning. In this article, I use the term "punitive" to refer to a set of practices enabled by networked digital infrastructures that allow for the infliction, extension, or intensification of sanctions—formal or informal—beyond conventional legal boundaries. In this context, punitiveness denotes not merely attitudes or penal severity, but the capacity of these infrastructures to generate, circulate, and sustain reputational, economic, or social harm through user participation. In other words, it captures how digital systems allow punishment to be enacted, amplified, and prolonged without state involvement or oversight.

Drawing on three cases—publicly accessible criminal records, informal reputational platforms, and the sharing of viral videos—the article examines how the mesh operates and why it poses novel challenges for justice, punishment, privacy, and the dynamics of social relations. Ultimately, it argues that the punitive mesh does not simply constitute an intensification of pre-existing trends but a qualitative shift toward a condition in which punishment is perpetual, mutual, and inextricable from the infrastructures of everyday communications and interactions. This marks more than a change in punitive practices —it signals a fundamental reconfiguration of social life itself. The punitive mesh suggests a new way of living with one another: in a constant state of being watched, judged, sanctioned, and archived across uncoordinated yet easily searchable online repositories and environments.

Theoretical lineage of the punitive mesh

My analysis draws on a series of influential theoretical accounts that, over several decades, have traced the evolution of control dynamics within the penal field and beyond.

Michel Foucault's *Discipline and Punish* (1995 [1975]) traces the transformation of punishment in the late eighteenth and nineteenth centuries from a sovereign model—centered on the spectacular and violent assertion of the ruler's power—to a disciplinary model in which control is exercised through constant surveillance. Public executions and corporal punishment give way to incarceration, regimented labor, and the meticulous regulation of time, space, and movement. The goal is not merely to inflict pain but to produce "docile bodies" that internalize certain norms and behave accordingly. The Panopticon—Jeremy Bentham's design for a prison in which inmates can be observed without knowing when they are being watched (see Bentham, 1995)[4]—serves for Foucault as the emblem of disciplinary power. The Panopticon does not require the actual, constant gaze of the guard but the mere possibility of observation. This uncertainty induces self-regulation, making overt coercion unnecessary. Over time, Foucault argues, this logic "escaped" the prison and permeated other institutions and settings—schools, factories, hospitals—producing a "carceral continuum" (Foucault, 1995 [1975]: 297, 303) in which surveillance is embedded in ordinary life. Closed institutions serve as "laboratories" where disciplinary techniques are developed, fine-tuned, and normalized. Once established, these techniques radiate outward into broader social settings and practices. As a result, control is exercised in open, everyday environments as much as in closed ones.

In most of the examples provided in *Discipline and Punish*, a distinction exists between watchers and watched; the subject of surveillance is not also the agent of it, and the positions are, for the most part, fixed. In his subsequent work, however, Foucault (1978 [1976], 1991) presents a more nuanced view of surveillance and control, less about institutions and fixed positions and more about a relational power that circulates through society, where individuals also participate in their own surveillance. This evolution sets the stage for Gilles Deleuze's concept of "societies of control" (1992), in which power becomes more decentralized and is exercised through flexible and subtle mechanisms, making control more pervasive and harder to resist. These dynamics help us understand the way in which, in the model of the punitive mesh that I will shortly outline and discuss, surveillance and punishment now operate laterally and diffusely, without any institutional mediation and in reciprocal fashion.

Stanley Cohen's *Punitive city* (1979) expands and develops the Foucauldian conceptual model from a punishment perspective. Observing the rise of community-based sanctions, halfway houses, and other alternatives to incarceration, Cohen argues that the carceral logic was dispersing into everyday life and beyond rigidly institutionalized contexts. In his account, the prison is no longer a sealed container of punishment; it is only one node in a network of control. Just like in Foucault, social control extends beyond the prison walls, reaching into the routines of daily life through probation, parole, community service, and new monitoring technologies, shifting from the prison to various community sites. This dispersal is accompanied by a marked blurring of boundaries: spatial boundaries and

distinctions between the imprisoned and the free, the guilty and the innocent, begin to blur; penal logic can now be found on street corners, in halfway houses, and in workplaces.

Cohen also describes how private actors are co-opted into the formal penal apparatus. Besides private entities, citizens are also mobilized as active participants in monitoring and controlling others through neighborhood watches, citizen patrols, and volunteer schemes, embedding punitive sensibilities into the fabric of civic engagement. The punitive city thus describes an expansion of penal control, both in geography and in the range of actors involved. While Foucault offers the theoretical model of how dynamics of surveillance, normalization, and control circulate beyond formal institutions into broader society, shaping how people behave, interact, and even think, Cohen shows us the outcome within the penal field. The punitive city is a spatial metaphor depicting the diffusion of penal power into different key aspects of social life. It highlights how penal measures expand and multiply, widening and thinning the net of control so that punishment saturates everyday social spaces beyond pre-defined sites. The dispersal of penal control across society is central to my analysis of the punitive mesh. The punitive city, however, still presupposes a certain degree of formal coordination: the state retains its central role in defining offenses, authorizing and imposing sanctions, and structuring relationships between the punisher and the punished. Community members and private actors may act as auxiliaries, but they do so within a penal framework anchored in law and formal punishment.

Four decades after Cohen, Shoshana Zuboff, in her book *The Age of Surveillance Capitalism* (2019), offers a different account of surveillance, one centered not on the penal system but on the economic logic of the digital age. Surveillance capitalism, she argues, is a novel form of market power in which personal data are extracted as "behavioral surplus" (Zuboff, 2019: 74–79) and used to predict—and ultimately shape—future behavior. This process is driven not by state imperatives but by corporate incentives: the monetization of attention, engagement, and predictive accuracy. Zuboff identifies key dynamics of surveillance capitalism, where devices, platforms, and services continuously extract behavioral data to anticipate and shape individual and group actions. Through predictive modeling and personalized interventions, users are nudged toward profitable behaviors, while the underlying logic of data capture remains opaque—creating a profound asymmetry of knowledge.

Unlike Foucault's disciplinary model, which aims to produce obedient citizens for the state, or Cohen's framework that disperses penal authority into the community, surveillance capitalism converts human experience into proprietary data streams for competitive advantage. The subject becomes both consumer and data source, with surveillance that is automatic, often imperceptible, and largely tolerated rather than chosen, built into the very conditions of participation. While Cohen emphasizes non-state actors deputized into a penal logic, Zuboff highlights their role as agents of a market-driven surveillance regime. Both Foucault and Zuboff examine how surveillance produces compliant subjects, but where Foucault sees compliance as normalizing and regulatory, Zuboff frames it as behavioral and consumptive. Her analysis of digital platforms—where behavior is continuously monitored, predicted, and modified—resonates with Deleuze's vision of control as decentralized, networked, and embedded in the infrastructures of everyday

life. Surveillance capitalism thus emerges as a concrete realization of Deleuze's theorization.

The next section defines the punitive mesh in detail, outlining its backdrop, core features, and the ways it reshapes both the reach and the nature of punishment in the digital age.

Defining the punitive mesh

The preceding discussion sets the stage for introducing the concept of the "punitive mesh." It is crucial to first emphasize how the contemporary landscape in which the mesh operates collapses distinctions that have traditionally structured the imposition and functioning of punishment.

(a) *State vs. private*: Public criminal records circulate on commercial platforms; private data infrastructures generate reputational proxies that influence state decision-making.
(b) *Watcher vs. watched*: The same individual may be a reviewer on a website or online app, a subject of review, a consumer of background checks, and a target of one.
(c) *Formal vs. informal*: Reputational harm may arise from an arrest record, a viral tweet, or a negative review, each potentially as damaging as the other, and often interconnected.
(d) *Economic vs. penal logic*: Platform incentives to maximize engagement often align with punitive impulses to expose, shame, and ostracize.

Crucially, what emerges is the aspect of peer-to-peer participation—a mode of social control in which ordinary individuals are both subjects and agents, where surveillance is incentivized by platform architectures, and where punitive outcomes emerge from the circulation of information irrespective of its legal status. The punitive mesh does not rely on an institutionalized gaze, a bounded urban metaphor, or a unidirectional flow of data for profit. It is a networked environment in which judgment, exposure, and censure are embedded in the infrastructures of everyday interaction. While users' practices sustain the punitive mesh, its very architecture is engineered by corporate actors whose design choices, data-extraction and dissemination models, and governance decisions make such participation consequential. Their role is central to understanding both how the mesh operates and why it has taken its current form.

The metaphor of the mesh aims to capture something essential about the present moment that neither the structure of the Panopticon nor the urban sprawl of the punitive city can fully represent. A mesh is not a tower, and it is not a set of streets radiating from a central square. It is diffuse and pervasive, but in a distinctive fashion. The mesh is a dense network of interconnected points, flexible yet inescapable. It has no singular center, no fixed direction of flow, no clear inside or outside. What defines the mesh is its *entanglement*: every node is connected to others, and the removal of any single node does not collapse the structure. The mesh is not anchored in a singular gaze or centralized authority,

but sustained through countless micro-interactions that collectively reinforce its configuration.

The punitive mesh therefore describes a form of social control in which surveillance, judgment, and sanction are embedded in the infrastructures of everyday life, enacted by a multiplicity of actors, and circulated through interconnected digital and physical spaces. Unlike traditional punishment, which is episodic and institutionally bounded, the punitive mesh operates continuously and without territorial limits. Its punishment is not necessarily codified in law, nor is it administered exclusively by state agents. Instead, punitive effects emerge from the persistent circulation of information—verified or alleged—about individuals' conduct, character, or identity. Importantly, the punitive mesh doesn't rely on evidentiary or procedural rules: rumors, innuendo, conjectures, distortion, and outright lies frequently serve as the primary forms of currency.

Core features of the punitive mesh

At least five core features characterize the punitive mesh:

1. *Mutual surveillance*: The mesh is characterized by the active participation of ordinary individuals as both watchers and watched. Surveillance is no longer primarily an asymmetrical relation between an authority and a subject; it is a mutual condition. Users of neighborhood crime apps report suspicious activities, while at the same time being rated by rideshare passengers or scrutinized on dating apps and other online reputational platforms. Likewise, a user may post a warning online about someone, only to discover that someone else has posted about them in a different forum.
2. *Lateral and omnidirectional flow*: If the Panopticon symbolizes institutional surveillance and the punitive city symbolizes spatial dispersal, the punitive mesh in today's networked societies symbolizes connective entanglement. It is everywhere, and operates in all directions, all at once—its strands linking legal databases, social media feeds, review platforms, and local gossip into a single, continuous fabric. In the mesh, flows of information are lateral and omnidirectional. A reputational post or piece of information may be read by peers, algorithmically boosted to strangers, scraped by data brokers, and fed into background check services—all without the knowledge of the subject or the consent of the originator. There is no single pathway for dissemination; rather, the mesh facilitates the rapid circulation of information through multiple, overlapping channels.
3. *Hybrid formal–informal sanctioning*: In the mesh, the boundary between legal and extra-legal punishment is porous. A mugshot from a police arrest may appear on a commercial "people search" site alongside unverifiable allegations from a community forum. Employers may consider both when making hiring decisions, without distinguishing between state-verified and crowd-sourced information. This hybridization destabilizes traditional categories of justice: sanctions may be socially enforced but legally baseless, or legally authorized but socially amplified beyond proportion.

4. *Persistence and searchability*: The elimination of temporal limits on punishment is another key characteristic of the punitive mesh. In a pre-digital environment, reputational harm from gossip or local exposure often faded over time, while access to official records required effort and was sometimes time-limited. The mesh renders exposure permanent: search engines, cached pages, and data aggregation ensure that once information is online, it remains accessible indefinitely. Redemption, in this context, becomes less a matter of reforming oneself than of overcoming the permanent archive of one's past.
5. *Platform incentivization:* Surveillance and exposure are not neutral byproducts of communication technologies; they are often the intended outcomes of platform design. Engagement is monetizable, and conflict—particularly reputational conflict—drives engagement. Platforms may not explicitly promote punitive content, but algorithms favor material that provokes strong emotional reactions, which often includes denunciations, warnings, and shaming posts. The mesh is thus not only sustained by user participation but structurally incentivized by the economic imperatives of digital platforms.

Technological development is central to how the punitive mesh operates and expands,[5] building on what Foucault, and later Deleuze, described as the dispersal of disciplinary power through surveillance, normalization, and the embedding of continuous, decentralized systems of control into everyday life. In this context, the punitive mesh is not a spontaneous or incidental outcome of digital life but the product of deliberate choices concerning data extraction and the circulation and persistence of reputational information. Its emergence reflects the convergence of commercial incentives, technological affordances, and governance gaps rather than an inevitable evolution of punishment.

In the same way, the punitive mesh does not replace the punitive city; it incorporates and extends it. Cohen described how punishment spread from prison to community; the mesh describes how different nodes of punishment are interlinked into a real-time network. Dispersal suggests distinct sites—probation office, workplace, community service location—each exercising control within its own domain. Entanglement suggests that these sites are no longer distinct. Data from one flow into the other, and reputational judgments in one domain (dating, employment, social circles, economic transactions) influence outcomes in others. For example, an arrest record posted online may be indexed by a search engine, discovered by a potential landlord, discussed on a neighborhood forum, and cited in a workplace Slack channel—all within hours. In practice, from this angle, there is no clear separation between criminal justice consequences and social consequences; to a significant extent, they are co-produced and mutually reinforcing.

Power in the punitive mesh operates through distributed, relational, and infrastructurally mediated processes. What distinguishes the punitive mesh from the accounts discussed is that power operates through reciprocal entwinement: platforms, data infrastructures, and individuals co-produce reputational consequences in ways that no single actor controls. The mesh is therefore not only a site where power circulates but a configuration that continually regenerates power through participation, connectivity,

and automated visibility. Its distinctiveness lies in how punitive force emerges from the interaction of infrastructural logics and human judgement, producing sanctions that are continuous, ambient, and difficult to attribute. Power is exercised not only through users' actions but through the design of systems that determine what becomes knowable, searchable, and actionable within the mesh.

The mesh as infrastructure

The punitive mesh should be understood not only as a metaphor but as a literal infrastructure: an assemblage of databases, algorithms, network protocols, search functionalities, and user interfaces that enable constant surveillance and reputational assessment. Unlike the walls of a prison or the physical layout of a city, the mesh has no material presence, yet it becomes hyper-tangible within digital environments. Its boundaries are defined not by physical barriers but by connectivity. If one node in the network is removed—a mugshot site taken down, a forum deleted—the punitive function persists through other nodes. The mesh is resilient precisely because it is decentralized. This infrastructural quality means the mesh can operate without being steered by any single actor. No one designs the punitive mesh as a whole; it emerges from the cumulative effects of platform designs, user behaviors, legal regimes, and cultural norms. Once established, it becomes self-sustaining: users contribute information because others do, and platforms retain it because deletion is costly and engagement is profitable.

The mesh integrates punitive logics into virtually every domain—romantic life, commerce, neighborhood relations, and online communities. It is "capillary" (Foucault, 1978 [1976]: 84) in this respect. Moreover, the mesh intersects with surveillance capitalism, amplifying the dynamics described in Zuboff's analysis: it extracts data from criminal records, reputational platforms, and everyday behavior, and subsequently modifies conduct by shaping opportunities and social interactions, thereby extending punitive effects into social, economic, and civic life. In traditional systems, one can identify the punisher —the guard, the judge, the parole officer. In the mesh, punitive effects may arise from anonymous posts, automated algorithmic sorting, or the cumulative weight of dispersed micro-actions. Furthermore, there is no "outside" to the mesh. Even disengaging from digital life does not prevent others from posting about you or accessing records in your absence. Finally, the mesh's punitive outcomes—ranging from public shaming and job loss to eviction and social ostracism—are often imposed without due process, evidence standards, or the possibility of appeal.

Examples of mesh dynamics

If the punitive mesh can seem abstract when described in theoretical terms, its logics become apparent when examined through concrete examples. The mesh is not a hidden system operating in the shadows of formal justice; it is a visible, participatory, and often celebrated digital infrastructure of mutual monitoring and sanctioning. The following cases illustrate how the interplay of exposure, informal sanction, and cross-platform circulation operates without, and often beyond, the state.

Public criminal records

The punitive mesh is perhaps nowhere more discernible than in the fate of criminal records in the digital age. What once existed as a localized, largely inert archive—stored in courthouse filing cabinets, accessible only through bureaucratic process—has become a readily accessible, almost frictionless data stream. The legal principle of "open justice," intended to ensure accountability, has collided with the commercial and technical affordances of the internet, radically expanding the reach and function of criminal records. Previously, accessing records required effort and physical presence, which acted as a de facto privacy shield (Corda, 2016; Solove, 2002). Employers rarely consulted distant archives, neighbors were often unaware of minor convictions, and gossip faded without documentary reinforcement. Digitization has erased these buffers (Solove, 2007). Many jurisdictions now publish court dockets online, data brokers aggregate court, police, and incarceration data for sale to employers, landlords, insurers, and the general public, and search engines index criminal history information for universal access (Corda and Lageson, 2020; Jacobs, 2015; Lageson, 2020; Lageson and Corda, 2024; Lageson et al., 2021). U.S. tech platforms have successfully exported such practices globally through the gig economy (Rovira, 2023: 3). Subscription-based platforms market themselves as tools for safety and risk management, but they also cater to voyeuristic interest.

A vivid example is the commercial mugshot industry in the United States. Since the mid-2000s, websites have published arrest photos scraped from police sites, monetizing traffic while also offering paid removal services (Lee, 2018). Several U.S. states have passed laws attempting to curtail such practices, prohibiting the solicitation of removal fees or restricting the publication of arrest photos before conviction (Wesner, 2017). Yet the mugshot economy persists, often relocating offshore or operating through social media pages with lax content moderation. Even where legal interventions succeed in removing a particular site, the same images often survive in cached versions, mirror sites, or private archives, ready to resurface (Lageson, 2020; Stelloh, 2017). Some U.S. newspapers have begun deleting or editing old crime stories to give individuals a fresh start; nevertheless, digital traces often persist through archives, news aggregators, or social media reposting (Levin, 2025). The mesh ensures resilience: once an image enters the network, it is almost impossible to erase.

The mesh collapses distinctions central to criminal law. Arrests, convictions, and sealed or expunged records often coexist in aggregated search results, making formal cessation of punishment practically meaningless. Likewise, the line between "criminal" and "non-criminal" information blurs: a Google search may produce court records alongside Yelp reviews, LinkedIn profiles, and neighborhood posts, creating a composite public persona outside the subject's control. The criminal record becomes a form of content—clickable, shareable, and profitable. The economic logic of this commodification ensures that there are strong incentives to keep the data circulating, regardless of its accuracy or current relevance. Moreover, the commodification process severs the information from its legal and temporal context. A twenty-year-old misdemeanor, long irrelevant in law, may appear with equal prominence as a recent felony in a paid search report

(McElhattan, 2025; Roberts, 2011). What remains is a flattened, decontextualized narrative of wrongdoing (Ewald, 2023).

The open justice principle was conceived in a world where public access meant physical attendance at a trial or deliberate retrieval of paper records. In the mesh, where "public" means "instantly searchable by anyone," the principle's consequences have multiplied exponentially. The law has not fully reckoned with the fact that the *form* of public access can radically alter its *function*. What was once a means of ensuring that justice was seen to be done has become a mechanism by which punishment is perpetually re-inflicted. In the mesh's logic, a criminal record often functions as an anchor point from which other punitive narratives can radiate. An arrest record may be linked to news articles, social media posts, workplace rumors, or user-generated reviews; even unrelated allegations can be algorithmically or contextually tied to that record through search results, reinforcing a durable association between a given individual and criminality. The anchor holds, even as other details shift or fade. This anchoring effect contributes to what may amount to a reputational trap. And unlike the temporally bounded sentences of the punitive city, the mesh allows punishment to migrate across contexts indefinitely.

Reputational platforms

If criminal records illustrate the ability of the mesh to extend state-originated punishment indefinitely via participatory (mis)use, informal reputational platforms reveal that punishment no longer requires any state origin at all. The following discussion focuses on spaces such as Tea, Yelp, Google Reviews, and Glassdoor—platforms where accusations, warnings, and evaluations circulate without legal vetting, yet wield enormous punitive power. These platforms demonstrate that the mesh's punitive capability is no longer necessarily tethered to formal legal processes. In these environments, the logic of accusation, circulation, and participatory sanction operates without courtrooms, police reports, or statutory definitions of wrongdoing. Instead, punishment emerges from peer-to-peer disclosures, often mediated by platform architectures that reward virality, emotional charge, and repetition. The result is a mode of social control that is at once diffuse, deeply personalized, and by and large immune to the procedural safeguards that traditionally accompany the exercise of punitive power.

The rise of informal reputational platforms highlights how the punitive mesh extends and operates well beyond and often independently of state-administered punishment. In 2025, the app Tea Dating Advice reached the top of Apple's U.S. App Store (Bradley, 2025).[6] Marketed as a women-only "whisper network," Tea allows anonymous reviews of men, flagged with "red" or "green" markers, alongside tools such as reverse image search and background checks. Framed in the language of safety and solidarity, the app provides users with a space to warn others about harmful behavior (Donnelly, 2025; Hunter, 2025). Yet its design—anonymous submissions, minimal moderation, no corroboration—blurs the line between protective sharing, gossip, and reputational destruction. Like a decentralized tribunal, Tea enables judgments rendered without rights of response, contextualization, or exoneration.

Similar dynamics appear in local Facebook groups such as "Are We Dating the Same Guy?," which have proliferated internationally (Al-Othman, 2025; Casteel et al., 2023; Merrifield, 2025). Members share experiences to report potential red flags, creating what amounts to a semi-public reputational archive. Private online groups or encrypted channels function in much the same way, allowing women to share names, screenshots, and anecdotes. Although portrayed as protective, these warnings often become searchable, exportable, and enduring—informal dossiers circulating beyond their original context. Here, the mesh operates through porous boundaries between intimacy and publicity. Employer-review platforms like Glassdoor or Indeed exemplify another dimension. A negative review of exploitative management can damage a company's brand, functioning as an economic sanction without legal intervention. Conversely, anonymous accusations of misconduct against specific employees can follow them across jobs, affecting employability without judicial oversight.

These platforms act as parallel legal orders. They assess conduct, render verdicts, and impose sanctions—diminished opportunities, reputational damage, exclusion—without invoking formal authority. Procedural minimalism is often defended on the grounds that these are not "real" legal processes. Yet their effects—social ostracism, economic loss, lasting stigma—closely parallel formal punishment.

Informal systems do not simply host accusations; they shape them. Algorithms privilege outrage, encourage pile-ons, and foster self-reinforcing plausibility, even when initial claims are unverified. Widespread circulation further amplifies harm. This multiplier effect is compounded by the mesh's cross-platform permeability. A negative review on Glassdoor may be screenshotted and shared on LinkedIn; an accusation on Tea may migrate to TikTok, accompanied by speculative commentary from strangers. Each migration detaches the claim further from its source, making correction more difficult and amplifying its reach. It is important, however, to acknowledge that many informal reputational platforms emerge in contexts where formal systems have failed to provide protection—particularly for women, queer people, and other marginalized groups. In such spaces, the public warning serves as a countermeasure to institutional indifference or active harm. Apps like Tea or online groups like "Are We Dating the Same Guy?" are often motivated by a recognition that reporting sexual harassment or abuse through official channels is frequently slow, retraumatizing, or futile. The informal network becomes a form of mutual defense (Cherelus, 2025; Orchard and Chamberlain, 2023). Yet this ethical foundation coexists with a more ambivalent reality: the same tools that allow for protective warnings also allow for unsubstantiated character assassination. The mesh does not discriminate between justice-seeking and malice-driven uses; it is an infrastructure for both. The possibility of false or exaggerated claims is not a mere "flaw" in the system—it is an inevitable consequence of its design, which prioritizes frictionless publication over verifiable accuracy.

The broader trend reflects a shift from rating products to rating people. What began with Amazon stars or TripAdvisor rankings now evaluates coworkers, dates, and strangers. Uber and Airbnb institutionalize reciprocal reviewing, making reputational scores prerequisites for participation. A low rating may not lead to prison, but it can exclude individuals from jobs, housing, or networks. Unlike products, people cannot be

relaunched; their review history endures. In this context, privacy is not so much violated as rendered structurally obsolete. Participation in social and economic life now presupposes a level of openness to public evaluation, whether voluntary or coerced. Even those who abstain from social media or public self-disclosure may find themselves indexed in the mesh through other people's posts. The very existence of a searchable, shareable platform means that the absence of information can itself become a kind of reputational marker, inviting speculation. Moreover, the shift from "broadcast" to "networked" communication means that personal allegations can move through semi-private channels—group chats, closed Facebook groups, Discord servers—before erupting into public view. The mesh thrives on this interplay between closed and open circuits, making reputational damage both unpredictable in timing and difficult to contain once triggered. From the perspective of reputational platforms, the very same subjects who decry hyper-invasive technologies often serve as the mesh's most diligent operators, producing and circulating the data that sustain its capacity for social control and participatory sanctioning.

Viral videos

Thirdly, and finally, another clear illustration of the punitive mesh comes from the life cycle of viral shaming videos. In one widely discussed case, in 2020, a woman in Central Park called the police on a Black birdwatcher, falsely claiming he was threatening her. The incident, recorded on a smartphone and originally posted to then-Twitter, exploded across social media within hours. The Twitter video alone received tens of millions of views (Stewart, 2020; Walters, 2020). The video triggered widespread condemnation, led to the woman's employer terminating her contract, and permanently altered her public identity (Maslin Nir, 2020). What is significant here is not the debate over whether her actions warranted social sanction—though that debate was intense—but the process by which the mesh adjudicated her case. The video moved frictionlessly across platforms, with each repost layering new commentary, captions, and interpretations. Within days, it had accumulated the aura of a settled fact: the woman was the "Central Park Karen" (Armstrong, 2021). There was no court process, no formal conviction, yet the outcome was unmistakably punitive—loss of employment, death threats, social ostracism, and enduring reputational damage (Cooper, 2023; Maxouris, 2020).

Even if one accepts the moral legitimacy or justice of this particular sanction,[7] the mechanism through which it unfolded is the same mechanism that can (and does) operate in far more ambiguous cases. An example of this is evident in the much-publicized incident in which a woman filmed at a 2025 Coldplay concert with her boss had a private moment rapidly converted into widespread shaming (Miller, 2025). The viral spread of videos online illustrates how informal punishment becomes participatory. Each act of sharing, reposting, and commenting contributed to the women's public trials, transforming individual incidents into a collective judgment. What appears to be casual circulation of content is, in fact, the social infrastructure through which reputations are reshaped and sanctions delivered. In this way, cases such as those of the "Central Park Karen" and the woman filmed at the Coldplay concert are not aberrations but paradigmatic examples of

how, in networked digital environments, punishment is enacted through the cumulative weight of distributed participation.

Implications and futures: Living in the punitive mesh

In today's networked societies, visibility is simultaneously a condition of vulnerability and a currency of power; participation is both protective and punitive. A screenshot in a private chat can become a public scandal; a reputational platform can operate as a parallel criminal record; a hashtag campaign can trigger sanctions faster than any court proceeding. Because the mesh is sustained by voluntary contributions of information, it is more resilient than any purely coercive surveillance regime. Disconnection is technically possible but socially costly: to refuse participation is to risk invisibility in domains—dating, employment, activism—where visibility is a precondition for opportunity and safety.

As mentioned, crucially, the mesh erodes the boundary between formal and informal punishment. While many of its sanctions operate outside the law, they routinely intersect with formal consequences: an employer acts on an online accusation without investigation; a landlord refuses a tenant based on an unverified warning in a neighborhood group; police initiate contact based on viral footage rather than a filed complaint. This entanglement creates a feedback loop in which informal punitive acts gain legitimacy from institutional uptake, and institutions increasingly rely on informal channels as de facto intelligence systems.

The punitive mesh combines long-standing dynamics of stigma and collateral consequences of criminal justice involvement (Corda and Kaspar, 2022; Logan, 2013) with new features introduced by digital infrastructures: scale, persistence, searchability, cross-context portability, and automated circulation. Punishment has never been fully contained within institutions, but the mesh renders diffuse sanctions more visible, durable, accessible, and actionable, transforming their reach and intensity. Going even further, and drawing on Fourcade and Healy's (2024) analysis of the "ordinal society," the punitive mesh also participates in a broader restructuring of governance through practices of ranking, scoring, and cross-context data mobility. It does not merely extend the scope and magnitude of punishment but contributes to a reordering of social life in which individuals appear as portfolios of reputational indicators that travel across domains, shape opportunities, and pre-structure social relations. These circulating scores reshape not only how punishment operates but how people are positioned, evaluated, and related to one another.

From an analytical perspective, the mesh poses a particular challenge because its most troubling features are inseparable from its most valued ones. Like other forms of power discussed, the mesh is both repressive and productive. It produces identities, rankings, and behavioral expectations while simultaneously exposing individuals to reputational harm and exclusion. Some of its salient features—visibility, connectivity, and participation—are inextricably linked to the mechanisms that enable punitive amplification. The same participatory capacities that allow communities to expose abusive employers, dangerous individuals, or corrupt officials also facilitate misidentification, harassment, and

disproportionate sanctions. Efforts to constrain the mesh's harms—through platform moderation, privacy protections, or defamation law—are easily framed as suppressing its democratic potential. This tension ensures that the mesh remains politically durable even in the face of controversy.

To acknowledge the existence of the punitive mesh is to recognize that we are not simply observers of a new, composite infrastructure but active participants in its day-to-day operations. Every search, screenshot, repost, and review is a potential filament in the lattice; every act of visibility is a wager on how one will be read, archived, and possibly weaponized.[8] Unlike other regimes of control, the mesh does not primarily operate by imposing its gaze upon a reluctant public. Instead, it seduces, enlists, and normalizes participation, weaving the satisfaction of being informed, the thrill of exposure, and the moral urgency of collective protection into the same gestures that enforce its punitive functions.

The implications are profound. Formal justice systems were designed around the assumption that sanctions flow from identifiable, accountable actors through defined procedures. In the mesh, sanctions can originate from anywhere, with no clear jurisdictional home, and yet yield tangible consequences. This destabilizes the traditional role of courts and regulators as both arbiters and safeguards: when punishment occurs before, outside, or without legal adjudication, the law is not merely circumvented but partially supplanted. The danger is not only wrongful harm but also a creeping redefinition of justice as something measured by virality and resonance rather than deliberation and proportionality. Capers (2023: 1768) suggests that "a world in which all of us can participate in the virtual town square and express our views about what is right and what is wrong—rather than leaving such decisions to those already in power—would be a brave new world indeed." Yet this participatory element is not necessarily desirable; diffusing responsibility for punishment to the crowd risks, as we can already see happening, amplifying biases, entrenching inequalities, and replacing far-from-flawless state control with an even more volatile and unaccountable form of collective judgment. The punitive mesh also demands a reconsideration of responsibility. The distributive nature of punitive acts—fragmented across thousands of likes, shares, and minor disclosures—makes it easy for individuals to disavow their role in producing harm. Yet, taken collectively, these micro-contributions generate a force that can be as impactful as any court ruling.[9] The mesh thrives on this diffusion of accountability: no single actor owns the sanction, but everyone contributes to its weight.

Privacy, long imagined as the antidote to invasive digital surveillance (Hildebrandt, 2019), becomes both more vital and more precarious in this environment. The mesh's power lies in its ability to mobilize personal data in service of certain narratives—narratives that may or may not correspond to legal or factual truth. Efforts to reclaim privacy, whether through encryption, anonymization, or digital clearance, confront not only technical challenges but also cultural resistance: assuming it is possible, withdrawal from visibility can be read as suspicious, antisocial, or even dangerous. The paradox deepens: the more we rely on mutual visibility, the more vulnerable we become to the punitive capacities that visibility enables. This vulnerability, however, is structured by the distribution of accountability across the mesh's multiple actors. While users play a crucial role in

perpetuating the mesh, corporate actors are central to its construction and operation. Individual participation is essential to its functioning, but platform infrastructures, social media companies, and data brokers shape the conditions under which reputational harm circulates. These actors determine the mesh's durability and opacity, making its punitive dynamics hard to challenge. Corporate actors not only produce and maintain the punitive mesh but also benefit from its operation, reinforcing the structural barriers that make it so difficult to confront.

Conclusion

This article has presented the concept of the "punitive mesh," highlighting how digital technologies have transformed punishment into a continuous, participatory, and networked form of social control. The punitive mesh illustrates how punishment and reputational harm, once confined to formal institutions, now circulate widely across interconnected online spaces, reshaping everyday life. In today's world, we inhabit an environment in which surveillance is not an exceptional intrusion but the medium of social existence, and punishment is not the endpoint of a legal process but a continuous possibility inherent in visibility itself. To live in the punitive mesh is to accept that one's public and private selves are not merely at risk of collapse—they are already largely entangled, circulating, and subject to judgment at every moment. This recognition does not demand resignation, but it does demand clarity.

Resistance to the mesh will require more than individual strategies of self-protection. Structural interventions are essential if we are to retain the democratic benefits of participatory exposure while mitigating its excesses. These could include targeted adjustments to ranking and recommendation systems to ensure punitive or harmful content is less readily amplified or made persistently visible, clearer limits on the circulation of sensitive data, and initiatives that foster more reflexive and accountable norms of online participation. Yet here the mesh's resilience presents a formidable obstacle. Its functions are distributed, its infrastructure privately owned but socially embedded, and its appeal rooted in values—transparency, accountability, and even solidarity—that are difficult to contest without appearing to defend impunity or concealment. The punitive mesh is not a passing cultural fad; it is an emergent infrastructure woven into the architecture of day-to-day existence. Its durability lies in its interweaving with the very freedoms and capacities—speech, association, participation, and mutual aid—that we are reluctant to relinquish. The challenge for the coming decades will be to imagine a civic order in which these freedoms are not the conduits of perpetual sanction. Until then, the punitive mesh will hold: elastic enough to manage dissent and disengagement, porous enough to absorb novelty, but always taut enough to catch, bind, and display those who stumble within it.

Acknowledgments

The author would like to thank Kevin Hearty, Robert Werth, and the two anonymous reviewers for their very helpful and insightful comments on earlier versions of this article.

ORCID iD

Alessandro Corda https://orcid.org/0000-0003-0220-2629

Funding

The authors disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: The author gratefully acknowledges support from a Barbara Huber Fellowship, awarded by the Max Planck Institute for the Study of Crime, Security and Law (Freiburg, Germany).

Declaration of conflicting interests

The author declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Notes

1. Solove (2021) argues that the "privacy paradox" is a myth because it wrongly generalizes from people's context-specific risk decisions to broad claims about their overall valuation of privacy. In other words, in his view, specific behaviors in limited scenarios do not accurately reflect general attitudes toward privacy. However, while context matters, persistent patterns of behavior—whether in surrendering personal data or evaluating others on platforms—can still provide meaningful evidence of how people assess and prioritize privacy, reputation, or other qualities, particularly when such behavior continues despite widespread warnings and awareness of potential risks.
2. We post pictures of us on holiday and share information about every aspect of our work, and about our personal and romantic lives via social media platforms. "Big tech" and social media wouldn't exist, never mind properly function, without the complicity of obliging users. Albrechtslund (2008) describes social media use in terms of "participatory surveillance," built around the ideas of user empowerment and subjectivity-building and sharing.
3. Cohen himself (1979: 346–347) uses the term "mesh" as a metaphor for the network or fabric of social control. Under his framework, "thinning the mesh" describes how this network becomes less intense or direct, dispersing punishment more subtly across society. It captures the shift from concentrated, overt control to diffuse, pervasive mechanisms of social regulation. The punitive mesh presented here is a dispersed and seemingly disordered network of social control, yet it maintains an underlying intensity when deployed. Its mechanisms are widespread and multifaceted, creating pervasive pressure. Wacquant (2012: 240) uses the term "punitive mesh" to describe how, in the 21st century, workfare and prisonfare operate as intertwined strategies of social control, linking neoliberal labor discipline with punitive criminal justice to regulate and manage marginalized populations.
4. The idea for the Panopticon was originally conceived by Samuel Bentham, Jeremy's younger brother, who envisioned a central inspection system for supervising workers efficiently (see Steadman, 2012).
5. Science and technology studies (STS) (e.g. Bowker and Star, 1999; Gillespie, 2014) help highlight how the punitive mesh is embedded in socio-technical systems that mediate visibility, classification, and data circulation. This literature underscores that the functioning and effects of the

mesh are inseparable from the technological and organizational arrangements that enable data to move, persist, and acquire meaning.

6. Later in the year, the app was taken down following multiple data-leak incidents, though it remained available on the Android app store. A new website was subsequently launched (Parham, 2026).
7. One person's punitive mesh—originating, for example, from #MeToo or cancel culture campaigns—is another person's form of citizen-led justice; this article does not seek to enter that broader debate.
8. Echoing debates in narrative criminology and storytelling literature (e.g. Maruna, 2025), individuals may choose to share personal accounts or curate digital self-representations, yet they retain little control over how these narratives are interpreted, appropriated, or weaponized by others. This dynamic resonates with the logic of the punitive mesh, in which content intended as benign—such as a TikTok video of a family outing—may be recontextualized to invite moral judgment or public shaming.
9. Furthermore, public awareness of wrongdoing in our contemporary landscape often emerges more rapidly via social media and gossip platforms than through formal court reporting. While courts typically release identifying details during official proceedings, digital channels frequently circulate such information from the moment of incident or arrest, reshaping the temporal and spatial dynamics of public exposure.

References

Albrechtslund A (2008) Online social networking as participatory surveillance. *First Monday* 13(3). https://doi.org/10.5210/fm.v13i3.2142.

Al-Othman H (2025) 'Are we dating the same guy?': Women turn to Facebook to uncover cheating and violence. *The Guardian*, February 1. Available at: https://www.theguardian.com/society/2025/feb/01/are-we-dating-the-same-guy-women-turn-to-facebook-to-uncover-cheating-and-violence.

Ambrose ML, Friess N and Van Matre J (2012) Seeking digital redemption: The future of forgiveness in the internet age. *Santa Clara Computer & High Technology Law Journal* 29(1): 99–164.

Andrejevic M (2004) The work of watching one another: Lateral surveillance, risk, and governance. *Surveillance & Society* 2(4): 479–497.

Andrejevic M (2006) The discipline of watching: Detection, risk, and lateral surveillance. *Critical Studies in Media Communication* 23(5): 391–407.

Armstrong M (2021) From lynching to Central Park Karen: How white women weaponize white womanhood. *Hastings Women's Law Journal* 32(1): 27–52.

Bennett CJ (2018) The European General Data Protection Regulation: An instrument for the globalization of privacy standards? *Information Polity* 23(2): 239–246.

Bentham J (1995) *The Panopticon Writings* (Božovič M, ed). London: Verso.

Birch K and Bronson K (2022) Big tech. *Science as Culture* 31(1): 1–14.

Bowker GC and Star SL (1999) *Sorting Things Out: Classification and Its Consequences*. Cambridge, MA: MIT Press.

Bradley S (2025) An app called Tea that lets women anonymously review guys has soared to No. 1 in the App Store. *Business Insider*, July 24. Available at: https://www.businessinsider.com/tea-app-women-share-anonymous-dating-reviews-goes-viral-2025-7.

Brayne S (2022) The banality of surveillance. *Surveillance & Society* 20(4): 372–378.

Capers IB (2023) Punishment without the state. *University of Illinois Law Review* 2023(5): 1753–1770.

Casteel DM, Leiser S and Papacharissi Z (2023) "Are we dating the same guy?": Collective sensemaking as a moral responsibility in Facebook Groups. *AoIR Selected Papers of Internet Research*. https://doi.org/10.5210/spir.v2023i0.13406.

Cherelus G (2025) Women have always looked out for one another. It's never been risk-free. *New York Times*, August 2. Available at: https://www.nytimes.com/2025/08/02/style/tea-app-data-breach-women-dating.html.

Chia SC (2020) Seeking justice on the web: How news media and social norms drive the practice of cyber vigilantism. *Social Science Computer Review* 38(6): 655–672.

Christiaens T (2025) Trust and power in Airbnb's digital rating and reputation system. *Ethics Information Technology* 27: 18.

Cohen S (1979) The punitive city: Notes on the dispersal of social control. *Contemporary Crises* 3(4): 339–363.

Cooper A (2023) I was branded the 'Central Park Karen'. I still live in hiding. *Newsweek*, November 7. Available at: https://www.newsweek.com/i-was-branded-central-park-karen-i-still-live-hiding-1839483.

Corda A (2016) More justice and less harm: Reinventing access to criminal history records. *Howard Law Journal* 60(1): 1–60.

Corda and Kaspar J (2022) Collateral consequences of criminal conviction in the United States and Germany. In: Ambos K et al. (eds) *Core Concepts in Criminal Law and Criminal Justice*. Vol. 2. Cambridge: Cambridge University Press, 392–437.

Corda A and Lageson SE (2020) Disordered punishment: Workaround technologies of criminal records disclosure and the rise of a new penal entrepreneurialism. *British Journal of Criminology* 60(2): 245–264.

Cubellis MA, Evans DN and Fera AG (2018) Sex offender stigma: An exploration of vigilantism against sex offenders. *Deviant Behavior* 40(2): 225–239.

Deleuze G (1992) Postscript on the societies of control. *October* 59: 3–7.

Donnelly D (2025) What is Tea – the women-only app with millions of users? *Sky News*, July 31. Available at: https://news.sky.com/story/what-is-tea-the-women-only-app-with-millions-of-users-13401888.

Ewald AC (2023) "You can't punish people for the rest of their life for something that they learned from, and changed from": Collateral consequences, inclusion, and narratives of responsibility. *Qualitative Sociology* 46(3): 375–401.

Foucault M (1978 [1976]) *The History of Sexuality. Volume I: An Introduction* (trans. Hurley R). New York: Pantheon Books.

Foucault M (1991) Governmentality. In: Burchell G, Gordon C and Miller P (eds) *The Foucault Effect: Studies in Governmentality*. Chicago: University of Chicago Press, 84–104.

Foucault M (1995 [1975]) *Discipline and Punish: The Birth of the Prison* (trans. Sheridan A). New York: Vintage Books.

Fourcade M and Healy K (2024) *The Ordinal Society*. Cambridge, MA: Harvard University Press.

Gallagher RJ, Stowell E, Parker AG, et al. (2019) Reclaiming stigmatized narratives: The networked disclosure landscape of #MeToo. *Proceedings of the ACM on Human-Computer Interaction* 3(CSCW): 1–30.

Gillespie T (2014) The relevance of algorithms. In: Gillespie T, Boczkowski PJ and Foot KA (eds) *Media Technologies: Essays on Communication, Materiality, and Society*. Cambridge, MA: MIT Press, 167–194.

Gilliom J and Monahan T (2012) *SuperVision: An Introduction to the Surveillance Society*. Chicago: University of Chicago Press.

Haggerty KD and Ericson RV (2000) The surveillant assemblage. *British Journal of Sociology* 51(4): 605–622.

Hildebrandt M (2019) Privacy as protection of the incomputable self: From agnostic to agonistic machine learning. *Theoretical Inquiries in Law* 20(1): 83–121.

Hunter T (2025) The Tea app lets women review their dates. Men are worried. *Washington Post*, July 24. Available at: https://www.washingtonpost.com/technology/2025/07/24/tea-dating-app-women-review-men/.

Ingber AS (2025) Understanding screenshot collection and sharing on messaging platforms: A privacy perspective. *Journal of Computer-Mediated Communication* 30(1): zmae023.

Jacobs JB (2015) *The Eternal Criminal Record*. Cambridge, MA: Harvard University Press.

Johnston L (1996) What is vigilantism? *British Journal of Criminology* 36(2): 220–236.

Kennedy L and Coelho M (2022) Security, suspicion, and surveillance? There's an app for that. *Surveillance & Society* 20(2): 127–141.

Lageson SE (2020) *Digital Punishment: Privacy, Stigma, and the Harms of Data-Driven Criminal Justice*. New York: Oxford University Press.

Lageson SE and Corda A (2024) Chasing a clean slate: The shifting roles of privacy and technology in criminal record expungement law and policy. *Harvard Journal of Law & Technology* 38(1): 1–47.

Lageson SE and Kaplun K (2021) Public accusation on the internet. In: Deflem M and Silva DMD (eds) *Media and Law: Between Free Speech and Censorship*. Sociology of Crime, Law, and Deviance. Bingley: Emerald Publishing, Vol. 26, 99–114.

Lageson SE and Maruna S (2017) Digital degradation: Stigma management in the internet age. *Punishment & Society* 20(1): 113–133.

Lageson SE, Webster E and Sandoval JR (2021) Digitizing and disclosing personal data: The proliferation of state criminal records on the internet. *Law & Social Inquiry* 46(3): 635–665.

Lee EK (2018) Monetizing shame: Mugshots, privacy, and the right to access. *Rutgers University Law Review* 70(3): 557–646.

Levin S (2025) US newspapers are deleting old crime stories, offering subjects a 'clean slate'. *The Guardian*, January 4. Available at: https://www.theguardian.com/us-news/2025/jan/04/newspaper-crime-stories.

Logan W (2013) Informal collateral consequences. *Washington Law Review* 88(3): 1103–1117.

Loveluck B (2019) The many shades of digital vigilantism. A typology of online self-justice. *Global Crime* 21(3–4): 213–241.

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

Maruna S (2025) Redeeming desistance: From individual journeys to a social movement. *Criminology; An Interdisciplinary Journal* 63(1): 5–25.

Marx GT (2016) *Windows into the Soul: Surveillance and Society in an Age of High Technology*. Chicago: University of Chicago Press.

Maslin Nir S (2020) How 2 lives collided in Central Park, rattling the nation. *New York Times*, June 14. Available at: https://www.nytimes.com/2020/06/14/nyregion/central-park-amy-cooper-christian-racism.html.

Maxouris C (2020) Christian Cooper is asking people to stop making death threats against the woman who called the cops on him. *CNN News*, May 27. Available at: https://edition.cnn.com/2020/05/27/us/amy-cooper-central-park-call-police-trnd.

McElhattan D (2025) Life sentences and minor offenses: Benchmarking, recalibration, and the culture of collateral consequence reform. *Law & Policy* 47(2): e70000.

Merrifield R (2025) Dark side of 'Are We Dating the Same Guy' Facebook groups where 'cheaters' are unmasked – but who are the REAL victims? *The Sun*, May 26. Available at: https://www.thesun.co.uk/news/35067105/toxic-facebook-groups-posting-lies/.

Miller L (2025) The ritual shaming of the woman at the Coldplay concert. *New York Times*, December 18. Available at: https://www.nytimes.com/2025/12/18/style/coldplay-concert-couple-kiss-cam-woman.html.

Murphy DS, Fuleihan B, Richards SC, et al. (2011) The electronic "scarlet letter": Criminal background and a perpetual spoiled identity. *Journal of Offender Rehabilitation* 50(3): 101–118.

Nissenbaum H (2004) Privacy as contextual integrity. *Washington Law Review* 79(1): 119–157.

Nowicki C (2024) Use Rate My Professors at your own risk. *The Daily Emerald*, May 24. Available at: https://dailyemerald.com/148470/opinion/nowicki-use-rate-my-professors-at-your-own-risk/.

Oguafor IV and Nevzat R (2023) "We are captives to digital media surveillance" Netizens awareness and perception of social media surveillance. *Information Development* 41(2): 465–478.

Orchard T and Chamberlain E (2023) Are we dating the same guy? Online groups toe the line between protecting women and defaming men. *The Conversation*, October 4. Available at: https://theconversation.com/are-we-dating-the-same-guy-online-groups-toe-the-line-between-protecting-women-and-defaming-men-214635.

Parham J (2026) The Tea app is back with a new website. *Wired*, January 15. Available at: https://www.wired.com/story/the-tea-app-is-back-with-a-new-website/.

Parker M and Dodge M (2024) The new neighborhood watch: An exploratory study of the Nextdoor app and crime narratives. *International Journal of Criminology and Sociology* 13: 43–54.

Payne WB (2024) Review bombing the platformed city: Contested political speech in online local reviews. *Big Data & Society* 11(3). https://doi.org/10.1177/20539517241275879.

Reosti A, Kurwa R and Bartram R (2024) Rental housing and the continuum of carcerality. *Theoretical Criminology* 28(4): 534–553.

Roberts J (2011) Why misdemeanors matter: Defining effective advocacy in the lower criminal courts. *UC Davis Law Review* 45(2): 277–372.

Rovira M (2023) The global rise of criminal background checks. *International Criminology* 3(1): 1–11.

Solove DJ (2002) Access and aggregation: Public records, privacy, and the constitution. *Minnesota Law Review* 86(6): 1137–1218.

Solove DJ (2007) *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet*. New Haven, CT: Yale University Press.

Solove DJ (2021) The myth of the privacy paradox. *George Washington Law Review* 89(1): 1–51.
Steadman P (2012) Samuel Bentham's Panopticon. *Journal of Bentham Studies* 14(1): 1–30.
Stelloh T (2017) Innocent until your mug shot is on the internet. *New York Times*, June 3. Available at: https://www.nytimes.com/2017/06/03/opinion/sunday/innocent-until-your-mug-shot-is-on-the-internet.html.
Stewart N (2020) The white dog walker and #LivingWhileBlack in New York City. *New York Times*, May 30. Available at: https://www.nytimes.com/2020/05/30/nyregion/central-park-video.html.
Strahilevitz LJ (2008) Reputation nation: Law in an era of ubiquitous personal information. *Northwestern University Law Review* 102(4): 1667–1738.
Tadelis (2016) Reputation and feedback systems in online platform markets. *Annual Review of Economics* 8: 321–340.
Taylor (2002) State surveillance and the right to privacy. *Surveillance & Society* 1(1): 66–85.
Trottier D (2017) Digital vigilantism as weaponisation of visibility. *Philosophy & Technology* 30(1): 55–72.
Wacquant L (2012) The wedding of workfare and prisonfare in the 21st century. *Journal of Poverty* 16(3): 236–249.
Walters J (2020) Video of white woman calling police on black man in Central Park draws outrage. *The Guardian*, May 26. Available at: https://www.theguardian.com/us-news/2020/may/26/central-park-new-york-white-woman-black-birdwatcher.
Wesner KL (2017) A reputation held hostage? Commercial mug shot web sites and the trade in digital shame. *Communication Law and Policy* 22(4): 459–495.
Zuboff S (2019) *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs.

Alessandro Corda is Reader in Criminal Law in the School of Law at Queen's University Belfast. His research focuses on the formal and informal collateral consequences of criminal justice involvement, comparative penal policies and practices, U.S. penal exceptionalism, and the sociology of punishment.