Logs and Hacks: Amazon, Surveillance, and Hacking as Epistemic Practice

Bruno Ministro
brunominstro@hackingthetext.net
Polytechnic Institute of Beja
Beja, Portugal
https://orcid.org/0000-0002-7147-3468

Abstract

This article examines how artistic interventions expose and contest Amazon's entanglement with surveillance, platform capitalism, and the politics of data. Focusing on *Ring™ Log* (2019) by Mark Sample and *Dear Jeff Bezos* (2013) by Johannes P Osterhoff, I analyze how these works use speculative and hacktivist tactics to reveal the ideological programs embedded in Amazon's products and services. Sample's piece stages a parody of automated neighborhood surveillance through pseudo-logs of Ring smart doorbells, foregrounding how machine vision and language transform everyday life into exportable incident data. Osterhoff's performative work turns a hacked Kindle into a device that emails reading activity directly to Amazon's CEO, thus exaggerating and exposing the invisible data extraction mechanisms in proprietary e-readers. Read together, these works illustrate a defiant, procedural critique that not only denounces digital surveillance but re-enacts its logics from within. Situating these interventions in relation to Amazon's broader infrastructural power —shaping the corporate web through innovations such as recommendation algorithms and cloud computing services— I argue that hacking emerges as more

than resistance: it is an epistemic practice, a way of knowing and making visible the extractivist logic of commercial technologies as they conquer our daily lives.

Keywords

Big Tech • Platform capitalism • Artivism • Hacktivism • Digital literature

Introduction

Today, the internet is so pervasive and intimate that it feels almost like an intranet. Yet, nothing about it is truly private. With or without users' explicit consent, web-based technologies regulate and monitor everyday life through global networked practices of online tracking, social profiling, and data extraction. What is more, as if this were not already alarming, most of this data is nowadays concentrated in the hands of just a few companies. These big tech firms, also known as tech giants or the big five, include Amazon, Alphabet (Google), Meta (Facebook), Apple, and Microsoft. Their concentration of power creates commercial monopolies that shape state decisions on public law, policy, and regulation.

Big tech and other companies benefit from data beyond the contexts and purposes for which it has been gathered. Data is precious in an increasingly digital world, and soft mechanisms for collecting user data are already the norm. Data is the new oil, as Clive Humby famously put it, and consequently, it is fueling all new sorts of businesses.

Artificial intelligence (AI) is one of the most visible examples of this today. The tech giants' quarterly public financial reports, as revealed by *The Guardian* in August 2025, show that they have collectively invested approximately $155 billion into AI development this year, already outpacing U.S. federal spending on education, training, employment, and social services in the 2025 fiscal year-to-date.[1]

As a 2023 report from AI Now Institute presciently demonstrated, it is no coincidence that big tech companies were the ones developing large language models at that crucial moment (Kak & West, 2023). Ultimately, only a handful of companies have the resources and capacity to build and sustain these technologies. And then, "whoever controls large language models controls politics" (Bajohr, 2023), as literary and AI scholar Hannes Bajohr notes in an article with the same name.

"Currently, the most urgent challenge," Christian Ulrik Andersen and Søren Bro Pold wrote over a decade ago, "is to get beyond the Google galaxy of controlled text, the Amazonic textual machinery, the infrastructures of controlled consumption" (Andersen & Pold, 2014, p. 185). And yet, everything that exists on the web today is mediated and controlled by just five big tech companies. In this context, my study addresses two interrelated questions: What is the relationship between emerging technologies, evolving business models, and users' perceptions of privacy and surveillance? How do artists and activists interpret and act upon these transformations and their social implications?

Over the past few decades, we have witnessed the creation of numerous literary and artistic digital works that critique data extractivism, digital surveillance and the erosion of privacy. These works provide a substantial and politically engaged corpus of digital artivism that seeks to uncover corporate unscrupulous practices and explore fairer alternatives. In this article, I explore the connections

[1] The tech giants' quarterly financial reports, as revealed by *The Guardian* in August 2025, show that they have collectively invested approximately $155 billion into AI development this year, already outpacing U.S. federal spending on education, training, employment, and social services in the 2025 fiscal year-to-date. https://www.theguardian.com/technology/2025/aug/02/big-tech-ai-spending (Last accessed 24 November 2025)

between art, society and big tech by first briefly reflecting on the corporate web as we know it today and then narrowing the focus to one of the companies already mentioned by Andersen and Pold: the "amazonian," almighty Amazon. Thus, section 1 is dedicated to contextualizing the intersection of the internet, control, and surveillance, with the following sections devoted to examining two critical-creative works that expose and counter this scenario.

The first example is *Ring™ Log* (2019) by U.S. electronic literature writer and scholar Mark Sample, an artivist speculation I analyze in section 2. The second is *Dear Jeff Bezos* (2013) by Johannes P Osterhoff, a German interface designer and artist whose hacktivist project I examine in section 3. By exploring these artivist speculations and tactical interventions around Amazon's Ring and Kindle, I aim to show how these particular products, when intervened and exposed by artists, make visible the embodied ideological program powered by Amazon's neoliberal agenda.

Other products that have been subject to many artistic interventions include Amazon Echo (and Alexa) and the Amazon online store itself. These feature prominently in works such as *The Listeners* (2015) by John Cayley and *The Hidden Life of an Amazon User* (2019) by Joana Moll. Both examples have been widely discussed, including in relation to surveillance. By narrowing my study to less-examined artistic works and supposedly less-troubled Amazon's products, I aim to test how the artistic hacks contribute to revealing the ideology underpinning Amazon's ecosystem as a whole.

The works' timeline is also relevant here. I chose to focus on a project released in 2019, right before the so-called AI boom in 2020, alongside another from 2013, a pivotal year for public awareness of mass digital surveillance following Snowden's revelations. This timeline is important because it demonstrates that creative hacking is a way of speculatively grasping systemic effects before they infiltrate more deeply into the social fabric and broader culture.

1. The Corporate Web

The so-called Web 2.0 is extractivist by design, with datafication being the primary driving force behind digital surveillance and control. Datafication refers to the transformation of social behavior into quantified data. States and corporations have been collecting vast amounts of online user-generated data, and they often collaborate on this process (Lefébure, 2014). As the Snowden case revealed in 2013, digital surveillance is not merely targeted at wrongdoers; we have all become objects of scrutiny through our online footprints. Roger Clarke first coined this as "dataveillance" (1988) and later described it as the "digital surveillance economy" (2019).

Recent scholarship has been devoted to the politics of big tech, either by offering detailed analyses of Amazon (West, 2022; Smith *et al.*, 2022) and Google (Graham, 2022), or by examining forms of resistance against digital platform capitalism and data colonialism (Bonini and Treré, 2024; Mejias and Couldry, 2024). Yet, to see the whole picture, one must remember that computer history and discourses have always relied on exploitative relations (Dyer-Witheford, 2015; Gray & Suri, 2019; Franklin, 2021; Whittaker, 2023).

The internet, in particular, functions as a pervasive surveillance network that operates on a global scale under the control of big tech. Some have described this as "surveillance capitalism" (Zuboff, 2019) and others as "platform capitalism" (Srnicek, 2017). Digital platforms work as 24/7 factories serving as an omnivorous space for generating, collecting and exploiting data as the new currency in the age of commodified information (Wark, 2019; Altenried, 2022). In fact, "with a long decline in manufacturing profitability," Nick Srnicek observes, "capitalism has turned to data as one way to maintain economic growth and vitality in the face of a sluggish production sector" (Srnicek, 2017, p. 11).

At first, the internet seemed to be about connection, and the web served as a space for freedom. However, that utopian idea has since been

questioned. It now seems clear that the internet is largely harnessed to sustain commodity fetishism (Crain, 2023). In a book that strikingly defines Distributed Denial of Service (DDoS) attacks as practices of civil disobedience, Molly Sauter notes that "the online space is being or has already been abdicated to a capitalist-commercial governance structure, which happily merges the interests of corporate capitalism with those of the post-9/11 security State while eliding democratic values of political participation and protest, all in the name of 'stability'" (Sauter, 2014, p. 150). In this context, the internet functions as a new mechanism, indeed, but one that repeats and even expands the neoliberal agenda into new realms. In doing so, it undermines the "promise of freedom" (Lessig, 1999, p. 6) attached to the internet in its early days, when it was supposedly characterized by "an inability to control" (1999, p. 147).

Early utopian visions of the internet as a democratic space with no centralized power structures for controlling its users have been challenged by robust criticism from media scholars (Galloway, 2004; Chun, 2006; Morozov, 2011; Lanier, 2014). For Alexander R. Galloway in particular, "the founding principle of the Net is control, not freedom" (2004, p. 142). Galloway's bold statement —central to his book *Protocol: How Control Exists After Decentralization*— relies on an in-depth analysis of the internet's technical protocols (TCP/IP, DNS, HTML, etc.) alongside earlier philosophical discussions from Foucault and Deleuze to Hardt and Negri. In Galloway's view, control was there from day one because "control is endemic to all distributed networks that are governed by protocols" (2004, p. 141).

To face this reality, Tiziana Terranova (2004) argued that network culture requires the development of micropolitical tactics that can effectively resist forms of social control. In line with this, Geert Lovink (2002) has long maintained that another internet is possible. For the internet culture critic, the "new" internet would only need to be based on decentralization, free software, and sustainable social networks. More recently, however, Lovink has reframed this perspective, contending that we are on the verge of witnessing the extinction of the internet, as, in his view, there is really no other way around it (Lovink, 2022). Similarly, Terranova's earlier optimism has shifted into a description of how we live in an age that already comes "after the internet" (Terranova, 2022). Taken together, these shifts suggest that even some of the most hopeful visions of a different web have run into a dead end —whether by invoking its "extinction" or by declaring that we live "after the internet". How could we have come to this?

As both a major player in the dotcom bubble of the 2000s and a dominant big tech company today, Amazon has played a decisive role in shaping the internet as we know it. Founded by Jeff Bezos in 1994 as an online bookstore, Amazon has since evolved into a leading e-commerce platform that sells a wide range of products. Amazon.com might well be "the Everything Store" (Stone, 2013), but Amazon Inc. is also a leader in many other business sectors, from online advertising to digital streaming and crowdsourcing. Perhaps more importantly, although less well-known, Amazon is the largest provider of cloud computing power through Amazon Web Services (AWS). Cloud computing includes the use of resources by different clients, for instance, for machine learning and AI deployment. Launched in 2006, AWS has consistently held the top position in the cloud computing market throughout recent years,[2] offering companies worldwide the infrastructure to develop their products and services. Amazon's biggest competitors in cloud computing are Microsoft Azure and Google Cloud, so everything remains in the hands of big tech at the end of the day.

In *Buy Now: How Amazon Branded Convenience and Normalized Monopoly*, Emily West (2022) defines Amazon as a retail platform, distribution infrastructure, media company, global "platform imperialist,"

[2] https://aag-it.com/the-latest-cloud-computing-statistics/ (Last accessed 24 November 2025)

and, above all, a deliberate and strategic shaper of affect and emotional responses. Writing for *The New Yorker* in 2014, journalist and writer George Packer recounts Amazon's history and, in doing so, makes clear that its mission has always been more about gathering consumer data than selling books or any other products (Packer, 2014). In recent years, several researchers in surveillance studies have argued that Amazon's objectives are not only commercial but also programmatic and ideological. Amazon, often described as "disruptive" in business jargon, invests in the rapid social infiltration of its technologies and practices, which, for Emily West, signals an intent to normalize surveillant logics among consumers (West, 2019). In a different yet related example, Justin Grandinetti claimed that Amazon's 2018 partnership with the United States' National Football League —introducing the adoption of real-time statistical analysis using Amazon Web Services and RFID tracking on the football field— was part of efforts "to normalize pervasive spatial data collection and analytics to a mass audience by presenting these surveillance technologies as helpful tools" (Grandinetti, 2019, p. 170).

In your spare time, besides watching a football game where analytics pop up incessantly in real time thanks to AWS servers' ping time, you can relax and watch a movie, listen to music, play a video game, or read a book without ever leaving Amazon's monopolistic playground. When you use Amazon's platform and its subsidiaries just for fun, you are also generating revenue for Jeff Bezos with your personal data —a practice that comes close to what media theorist Ian Bogost once labeled "hyperemployment" (Bogost, 2013).[3] This form of "working" as a user is now so deeply embedded in our social fabric that we barely notice it anymore.

In the introduction to *Amazon: At the Intersection of Culture and Capital*, editors Paul Smith, Alexander Monea and Maillim Santiago have pointed out that Amazon has not only changed the face of business but has also had a broader cultural impact on society. According to these scholars, Amazon's business model relies on its dominant market position and powerful infrastructure, but also, fundamentally, on the exploitation of an expanding global workforce. This is most visibly represented in the poor working conditions at various Amazon warehouses, which have repeatedly been brought into the spotlight in the news. It is also indirectly represented by the widely adopted crowdsourcing platform Amazon Mechanical Turk, where a global workforce performs tasks for minimal compensation and without labor rights. Finally, it is reflected in the "hyperemployment" of users who generate data that is collected, analyzed and sold as a form of non-consensual, unpaid, extractivist labor. Users are of great use.

2. Knock-Knock-Knockin' on Surveillance Door

With a mission to help make neighborhoods safer and give people peace of mind, Amazon's Ring home security cameras promise users security and control. Yet it is hard to see how anyone could feel reassured when their phone pings with a notification every time motion is detected at their front door —one of Ring's standard features.

The tool has sparked privacy concerns since its initial release in 2014 under the name of DoorBot, well before its official acquisition by Amazon four years later.[4] In 2019, Amazon's Ring was at the center of controversy for providing police with camera footage directly from users. After softening

[3] Further exploring Bogost's catchphrase, see Domenico Quaranta and Janez Janša's *Hyperemployment – Post-work, Online Labour and Automation*, a book that grew out of a year-long program in Ljubljana, which included exhibitions, a symposium, artist talks, and other satellite events. https://aksioma.org/hyperemployment (Last accessed 24 November 2025)

[4] Other Amazon devices —from Echo/Alexa to wearables like the Halo smartwatch— have raised similar privacy and surveillance concerns.

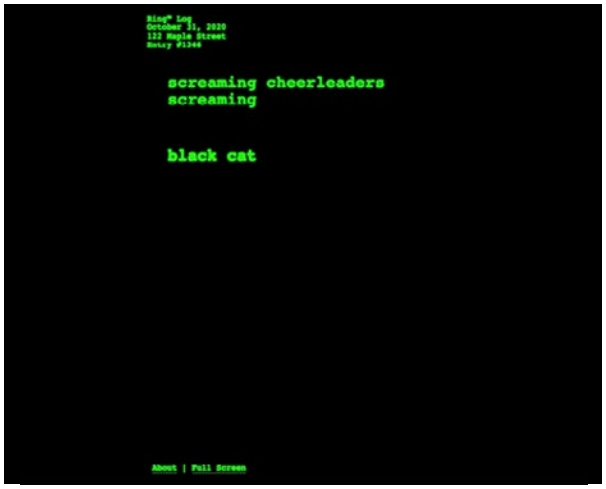

Figure 1. Mark Sample, *Ring™ Log* (2019). Source: fugitivetexts.net/ring

its public image for a couple of years, Ring now seems poised to return to its initial surveillance mode, as reported by *Business Insider*.[5] In an opinion piece published by the Electronic Frontier Foundation in August 2025, policy analyst Matthew Guariglia —who describes Ring as born out of a surveillance-first-privacy-last approach— argues that Ring is cashing in "on the rising tide of techno-authoritarianism, that is, authoritarianism aided by surveillance tech," also noting that "[t]oo many tech companies want to profit from our shrinking liberties" (Guariglia, 2025, np).[6]

Building on the public discussions that arose in 2019, Mark Sample created *Ring™ Log*.[7] This browser-based artwork stages a near-future scenario of smart domestic surveillance. The piece imagines what would happen if doorbell cameras used AI object detection to watch, interpret, and automatically log what they saw, particularly on a night when appearances defy easy categorization: Halloween.

Conceptually, Sample frames the project as "an experiment in speculative surveillance" —a "what if" exercise that parodies the tone and claims of smart-home security while probing its blind spots and failures. The premise is simple and sharp: when the AI attempts to label costumed bodies, its categories wobble, absurdities accumulate, and the log exposes how automated surveillance can naturalize suspicion, flatten nuance, and turn everyday life into a series of indexable incidents —especially when corporate platforms mediate neighborhood perception.

As we can see in Figure 1 —and as already encapsulated in the work's title— *Ring™ Log* is not about video footage but about the textual descriptions of imagined footage as detected by the device. A log, in its most general sense, is a record of events, activities, or data. In digital media, logging refers to the process of capturing and storing records of system activity, ranging from operational details to errors and other notable events (e.g., a console log).

Using HTML, CSS, and JavaScript, the work presents itself as a pseudo-log interface with old-school style green text on a black screen and scrambling text animation effects. Inspecting the source code reveals that the text is randomly pulled from a JavaScript array to display descriptions such as "robot and gorilla," "ghost," "miscellaneous superheroes," "Amazon Prime Delivery," and "the devil," along with error messages like "ERROR 775 DETECTION_ALGORITHM_FAILURE" and "ERROR 4377 OBJECT_DETECTION_DATA_BREACH."

By coding absurd categories and error codes, the work hacks surveillance logics and logistics, revealing the ideological investment embedded in products presented as beneficial and well-intentioned. The aesthetics of failure here are twofold. On the one hand, errors appear as text descriptions in the source code. On the other hand, the glitchy visuals of the

5 https://www.businessinsider.com/amazon-ring-founder-mode-jamie-siminoff-crime-fighting-roots-2025-7 (Last accessed 24 November 2025)

6 https://www.eff.org/deeplinks/2025/07/amazon-ring-cashes-techno-authoritarianism-and-mass-surveillance (Last accessed 24 November 2025)

7 https://fugitivetexts.net/ring (Last accessed 24 November 2025)

interface make those descriptors difficult to follow as they scramble into view and disappear again quickly. The interplay of both types of glitches produces a destabilizing critique of privatized surveillance as an interface of everyday life.

As I suggested earlier, one central aspect of Sample's work is that it adopts the log format rather than mimicking video footage. In this way, it foregrounds labels, timestamps, and metadata as aesthetic surface and rhetorical target. In doing so, it highlights the connection between two existing surveillance modes. The most visible is video surveillance —think of Ring as a CCTV camera, because it is; and recall that even today CCTV remains the most familiar mode of surveillance in our analog collective imaginary. The second mode involves digital tools and techniques for capturing, inspecting, and using data; this is speculatively represented in *Ring™ Log* through its textual logs. This mode of surveillance, therefore, is both *discrete* and *discreet*. It is discrete because it consists of binary units we call digital information (data points, data flows, etc.), and it is discreet because it is a form of surveillance that commits to remaining unnoticed.[8]

In this, *Ring™ Log* makes the connection between both modes of surveillance explicit by transforming pseudo-video captures into pseudo-textual logs. The role of language and form is central to this hack. Everything Ring logs on that Halloween night takes the form of a mediated description rather than reproduction. Sample's *Ring™ Log* weaponizes natural language, code, and the user interface as a critique of securitization.

It is worth noting that Mark Sample's speculation has since become reality: Ring doorbells now include AI-driven object detection. In 2021, Ring officially launched the "Smart Alerts" system, which relies on motion detection for package alerts and custom events. By 2025, Premium customers had beta access to a service called "Video Descriptions," which uses machine vision and generative AI to interpret objects and send notifications to users.[9]

In the next section of my article, I examine a different kind of log (and hack) —one that operates more silently behind the screens of Kindle e-readers, sending user data on a tour through Kindle's WhisperSync technology. Before that, however, I propose we "read" Kindle's Terms and Conditions.

3. Big Tech, Small Print (or just "I agree")

In *How Long Does It Take to Read Amazon Kindle's Terms and Conditions?*, a thought-provoking project led in 2017 by Australian consumer advocacy group Choice, the answer to the question came from an actor who read all 73,198 words of Kindle's Terms and Conditions aloud, taking almost nine hours to finish.[10] This case illustrates a broader problem: lengthy, jargon-laden contracts and end-user license agreements (commonly referred to as EULAs) are

[8] At this point, and as a side note, I would also like to mention Evan Light's research project "Deconstructing/Performing the Amazon Ring Security Apparatus," which connects surveillance, art, and media. Available at: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/funding-for-privacy-research-and-knowledge-translation/completed-contributions-program-projects/2022-2023/p_202223_03/ (Last accessed 24 November 2025)

[9] Sample was visionary in October 2019, but like all of us, he could not have imagined the coming of the COVID-19 pandemic a couple of months later —a period during which Amazon's delivery services saw nearly a 200% rise in profits. Still, Sample had the opportunity to develop a kind of Ring 2.0 during quarantine, explicitly focusing on the new scenario. *Ring™ Camera Pandemic Log* can be accessed at: https://fugitivetexts.net/quarantine/ (Last accessed 24 November 2025)

[10] A short description of *How Long Does It Take to Read Amazon Kindle's Terms and Conditions?* can be found at: https://theglassroom.org/object/choice_australia-how_long_does_it_take_to_read_amazon_kindles_terms_and_conditions/ (Last accessed 24 November 2025). A video summary of the painful nine-hour reading is available at: https://www.youtube.com/watch?v=sxygkyskucA (Last accessed 24 November 2025)

Figure 2. Johannes P Osterhoff, *Dear Jeff Bezos* (2013). Source: web.archive.org/web/20181225045810/http://bezos.cc

pervasive in the digital world, often discouraging informed consent and shielding companies from scrutiny. Because of their length and illegibility, such documents are routinely accepted by users without being read, raising concerns about transparency, fairness, and consumer rights.

Besides the ironic approach represented by Choice's project, there are also initiatives that try to help users navigate these unmanageable documents. For instance, *ToS;DR* is a community-led project launched in 2012 that summarizes and explains Terms of Service.[11] A quick search on the website shows that most services offered by big tech receive a grade E —the lowest on the scale. These include Amazon's Goodreads, IMDb, and the flagship online store; Meta's Facebook and Instagram; and Alphabet's YouTube and Google Search. Other poorly rated platforms include PayPal, Reddit, Alibaba, eBay, Uber, Merriam-Webster, WikiHow, and CNN, among many others.

The work I analyze next might well be considered a violation of Kindle's Terms and Conditions. In *Dear Jeff Bezos* (2013), artist Johannes P Osterhoff modified his Kindle e-reader to automatically send an email directly to Amazon's CEO each time the artist set a bookmark on his jailbroken device. At the same time, this activity was also made public online, as shown in Figure 2.[12] In a short interview for *Rhizome*, when asked for his motivations, Osterhoff replied: "Not so long ago it was very simple to read a book in private. With the Kindle and WhisperSync it is impossible. I am required to surrender my privacy during reading on my Kindle. So sending e-mails about my reading activity directly to the CEO of Amazon was just the next logical step" (Osterhoff, 2013b, np).[13]

Dear Jeff Bezos creates a persistent, humorous reminder of user activity and exposes the hidden data flows embedded in everyday digital media in general and in the Kindle device in particular. This occurs because Amazon's e-reader has a built-in program that logs Kindle user data and shares it with Amazon's servers through their WhisperSync technology. The data tracked by Amazon includes the books purchased and device information, but also data generated during usage, such as reading progress, annotations, highlights, dictionary look-ups, added notes, bookmarks, page turns, and last page read, among other user activities.

According to Kindle's Terms of Service, all of this data is used to sync content across devices and to feed Amazon's recommendation algorithms. Some of this information is also made public in a feature called "Popular Highlights," which shows other customers the most annotated passages in a book. As *The Guardian* reporter Kari Paul neatly summarized: "Amazon knows more than just what books I've read and when —it knows which parts of them I liked the most" (Paul, 2020).

[11] https://tosdr.org (Last accessed 24 November 2025)

[12] An archived version of the website containing all the emails sent to Bezos between 12 January 2013 and 12 January 2014 can be accessed at: https://web.archive.org/web/20181225045810/http://bezos.cc/ (Last accessed 24 November 2025)

[13] https://rhizome.org/editorial/2013/jan/12/dear-jeff-bezos/ (Last accessed 24 November 2025)

While Johannes P Osterhoff describes the project as an "online performance piece," it is clear that such provocative practice also belongs to the realm of hacktivism. A key aspect is that a Kindle device is jailbroken and hacked[14] not to bypass its inner mechanisms, but ironically to amplify its surveillance functions. In other words, Osterhoff does not intervene in his personal device to avoid the tracking of his reading habits; instead, he goes to extremes by sharing them publicly. In the same interview cited earlier, the artist states: "Companies like Amazon are interested in exclusive ownership of data, because with this exclusivity comes its value. [...] To make the data I generate public, is to devalue it" (Osterhoff, 2013b).

Equally important, this resonates with Scott Rettberg and Roderick Coover's observation that creative approaches like the one analyzed here "allow authors not only to critique aspects of the digital turn but to illustrate the object of critique procedurally within the systems themselves" (Rettberg & Coover, 2020, np). In this sense, Osterhoff's gesture clearly corresponds to what Alexander R. Galloway and Eugene Thacker call an "exploit." Borrowing the term from hacker parlance, they argue that "[p]rotocological struggles do not center around changing existent technologies but instead involve discovering holes in existent technologies and projecting potential change through those holes" (Galloway & Thacker, 2007, p. 81).

Of course, the most important layer in *Dear Jeff Bezos* is not the practical one, but the raising of general awareness alongside the fun. In this provocative work, the artist probes the hidden mechanisms behind Kindle's controlled-consumption interface, sparking dialogue about commercial strategies, their cultural impact and the position of users within these systems. And Osterhoff does so in a witty, tongue-in-cheek, hacktivist style.

I do not want to close this section without noting that —unlike Ring— Kindle has received considerable attention from artists and activists. Creative works that engage in often humorous experiments with the e-reader include the print-on-demand books *56 Broken Kindle Screens* (2012) and *Networked Optimization* (2015), both by Silvio Lorusso and Sebastian Schmieg. The first assembles photos found online depicting broken Kindle screens, while the second explores the "Popular Highlights" feature. Perhaps more widely discussed, *E-Book Backup* (2012) by Jesse England responds to the controversial 2009 incident when Amazon deleted George Orwell's *1984* and *Animal Farm* from every Kindle device without any explanation to its users.[15] Like *Dear Jeff Bezos*, all three examples encapsulate a straightforward reflection on privacy, digital transformation, and proprietary software —concerns we must engage if we want to better understand and counteract current modes of digital surveillance.

Conclusion

Customer reviews, one-click payments, free shipping, and personalization through an algorithmic recommendation system ("Customers like you also purchased..."), among others, were technological innovations pioneered by Amazon that gained traction and were later adopted by other digital-oriented businesses, greatly shaping the corporate web and its rules. My article leaves out many Amazon products and services and, as such, it does not serve as a personalized recommendation for readers' next purchase on the "Everything Store."

[14] In practice, the artist rooted his Kindle and wrote a PHP script that automatically sent a message to his server, which then forwarded it as an email to Bezos. See Osterhoff, 2013b.

[15] These and other provocative book projects around Amazon are documented on the Post-Digital Publishing Archive (https://p-dpa.net) and the Library of Artistic Print on Demand (https://apod.li), coordinated by Silvio Lorusso (P-DPA) and by Andreas Bülhoff and Annette Gilbert (APOD-Li), respectively. (Last accessed 24 November 2025)

Narrowing the scope of my analysis to Kindle and Ring allowed me to show how unruly artists and writers have been exposing Amazon as a natural target for countering platform capitalism and big tech influence. In this study, I proposed that Amazon's agenda becomes most visible in each of its products and services when artists tear them apart and hack them, both practically and imaginatively.

By creating pseudo-logs and imagining surveillant modes at the intersection of machine vision and language models, *Ring™ Log* operationalizes suspicion as syntax, revealing how implementation choices algorithmically narrativize neighbors and turn domestic and communal spaces into exportable incident data. With Ring doorbells now equipped with AI-powered analytical, archival, and dissemination capacities, Ring serves as a substitute for CCTV cameras, and it is no longer a "TV" or a "Closed Circuit." Ring's simple and "off-the-shelf" product is, in fact, a powerful multimedia, ubiquitous machine that openly logs, tags, and distributes recordings and metadata from our front doors potentially at a global scale through the internet.

Global connectivity is precisely what, at the most basic level, allows Amazon to access and continually sync readers' activities on Kindle. *Dear Jeff Bezos* ironically pushes these technical mechanisms forward to make them so visible that the reality becomes unbearable. What is at stake is not whether the artist gives away his privacy or whether Bezos really wants to know what this particular reader is reading. What is at stake is how, why, and for what ends Amazon seeks to control all readers and their activities in order to exploit that data for its own purposes.

Throughout history, both Amazon and other companies have often faced calls for boycotts in response to specific incidents or broader concerns. This approach has often been an important tactic for raising public awareness and fostering broader discussion around such issues. Nonetheless, looking at Sample's and Osterhoff's works as practices of hacktivism connected to the idea of the commons, I contend that hacking is more important than boycott alone. Creative hacking is a timely tactic that reveals the logic of systems as they emerge. Hacking is not only resistance but an epistemic practice: a way of knowing the system from inside and anticipating its wider cultural impact on society and everyday life.

Bibliographic references

[1] Altenried, M. (2022). *The Digital Factory: The Human Labor of Automation*. University of Chicago Press.

[2] Andersen, C. U., & Pold, S. B. (2014). Post-digital Books and Disruptive Literary Machines: Digital Literature Beyond the Gutenberg and Google Galaxies. *Formules/Revue Des Creations Formelles*, *18*, 164–183.

[3] Bajohr, H. (2023, April 8). Whoever Controls Language Models Controls Politics. *Hannes Bajohr*. https://hannesbajohr.de/en/2023/04/08/whoever-controls-language-models-controls-politics/

[4] Bogost, I. (2013, November 8). Hyperemployment, or the Exhausting Work of the Technology User. *The Atlantic*. https://www.theatlantic.com/technology/archive/2013/11/hyperemployment-or-the-exhausting-work-of-the-technology-user/281149/

[5] Bonini, T., & Treré, E. (2024). *Algorithms of Resistance: The Everyday Fight Against Platform Power*. The MIT Press.

[6] Chun, W. H. K. (2006). *Control and Freedom: Power and Paranoia in the Age of Fiber Optics*. The MIT Press.

[7] Clarke, R. (1988). Information Technology and Dataveillance. *Communications of the Association for Computing Machinery*, *31*(5), 498–512.

[8] Clarke, R. (2019). Risks Inherent in the Digital Surveillance Economy: A Research Agenda. *Journal of Information Technology*, *34*(1), 59–80. https://doi.org/10.1177/0268396218815559

[9] Crain, M. (2023). *Profit Over Privacy: How Surveillance Advertising Conquered the Internet*. University of Minnesota Press. https://doi.org/10.5749/9781452971667

[10] Dyer-Witheford, N. (2015). *Cyber-Proletariat: Global Labour in the Digital Vortex*. Pluto Press.

[11] Franklin, S. (2021). *The Digitally Disposed: Racial Capitalism and the Informatics of Value*. University of Minnesota Press.

[12] Galloway, A. R. (2004). *Protocol: How Control Exists After Decentralization*. The MIT Press.

[13] Galloway, A. R., & Thacker, E. (2007). *The Exploit: A Theory of Networks*. University of Minnesota Press.

[14] Graham, R. (2022). *Investigating Google's Search Engine: Ethics, Algorithms, and the Machines Built to Read Us*. Bloomsbury.

[15] Grandinetti, J. J. (2019). Welcome to a New Generation of Entertainment: Amazon Web Services and the Normalization of Big Data Analytics and RFID Tracking. *Surveillance & Society*, *17*(1/2), 169–175. https://doi.org/10.24908/ss.v17i1/2.12919
[16] Gray, M. L., & Suri, S. (2019). *Ghost Work: How to Stop Silicon Valley from Building a New Global Underclass*. Houghton Mifflin Harcourt.
[17] Guariglia, M. (2025, July 18). Amazon Ring Cashes in on Techno-Authoritarianism and Mass Surveillance. *Electronic Frontier Foundation*. https://www.eff.org/deeplinks/2025/07/amazon-ring-cashes-techno-authoritarianism-and-mass-surveillance
[18] Kak, A., & West, S. M. (2023). *AI Now 2023 Landscape: Confronting Tech Power*. AI Now Institute. https://www.ainowinstitute.org/2023-landscape
[19] Lanier, J. (2014). *Who Owns the Future?* Simon & Schuster.
[20] Lefébure, A. (2014). *L'affaire Snowden: Comment les États-Unis espionnent le monde*. La Découverte.
[21] Lessig, L. (1999). *Code and Other Laws of Cyberspace*. Basic Books.
[22] Lovink, G. (2002). *Dark Fiber: Tracking Critical Internet Culture*. The MIT Press.
[23] Lovink, G. (2022). *Extinction Internet*. Institute of Network Cultures.
[24] Mejias, U. A., & Couldry, N. (2024). *Data Grab: The New Colonialism of Big Tech and How to Fight Back*. The University of Chicago Press.
[25] Morozov, E. (2011). *The Net Delusion: The Dark Side of Internet Freedom*. PublicAffairs.
[26] Osterhoff, J. P. (2013a). *Dear Jeff Bezos*. https://web.archive.org/web/20181225045810/http://bezos.cc
[27] Osterhoff, J. P. (2013b, January 12). Interview by Ben Fino-Radin. *Rhizome*. https://rhizome.org/editorial/2013/jan/12/dear-jeff-bezos/
[28] Packer, G. (2014, February 9). Cheap Words. *The New Yorker*. https://www.newyorker.com/magazine/2014/02/17/cheap-words
[29] Paul, K. (2020, February 3). "They know us better than we know ourselves": How Amazon tracked my last two years of reading. *The Guardian*. https://www.theguardian.com/technology/2020/feb/03/amazon-kindle-data-reading-tracking-privacy
[30] Quaranta, D., & Janša, J. (Eds.). (2020). *Hyperemployment – Post-work, Online Labour and Automation*. NERO and Aksioma – Institute for Contemporary Art, Ljubljana.
[31] Rettberg, S., & Coover, R. (2020). Addressing Significant Societal Challenges Through Critical Digital Media. *Electronic Book Review*. https://doi.org/10.7273/1MA1-PK87
[32] Sample, M. (2019). *Ring™ Log*. https://fugitivetexts.net/ring
[33] Sauter, M. (2014). *The Coming Swarm: DDoS Actions, Hacktivism, and Civil Disobedience on the Internet*. Bloomsbury.
[34] Smith, P., Monea, A., & Santiago, M. (Eds.). (2023). *Amazon: At the Intersection of Culture and Capital*. Rowman & Littlefield.
[35] Srnicek, N. (2017). *Platform Capitalism*. Polity.
[36] Stone, B. (2013). *The Everything Store: Jeff Bezos and the Age of Amazon*. Bantam Press.
[37] Terranova, T. (2004). *Network Culture: Politics for the Information Age*. Pluto Press.
[38] Terranova, T. (2022). *After the Internet: Digital Networks Between Capital and the Common*. Semiotext(e).
[39] Wark, M. (2019). *Capital is Dead: Is This Something Worse?* Verso.
[40] West, E. (2019). Amazon: Surveillance as a Service. *Surveillance & Society, 17*(1/2), 27–33. https://doi.org/10.24908/ss.v17i1/2.13008
[41] West, E. (2022). *Buy Now: How Amazon Branded Convenience and Normalized Monopoly*. The MIT Press.
[42] Whittaker, M. (2023). Origin Stories: Plantations, Computers, and Industrial Control. *Logic(s) Magazine*. https://logicmag.io/supa-dupa-skies/origin-stories-plantations-computers-and-industrial-control/
[43] Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Profile Books.

Bio

Bruno Ministro is an Invited Adjunct Professor at the School of Technology and Management of the Polytechnic Institute of Beja. He holds a PhD in Materialities of Literature from the University of Coimbra. His current research topics focus on the automation of reading and writing, technological solutionism, and surveillance capitalism. The latest volumes he has edited include *Conceptual Writing, Experimental Poetry and Humor* (ILC Livros Digitais, 2024) and *Transformative Repetition in Experimental and Post-Digital Poetics* (Edinburgh University Press, 2026).

Artigo recebido em 2025-09-03

Artigo aceite em 2026-01-13

Artigo publicado em 2026-02-23

Ministro, B. (2026). Logs and Hacks: Amazon, Surveillance, and Hacking as Epistemic Practice. *Rotura – Revista de Comunicação, Cultura e Artes*, *6*(1). https://doi.org/10.34623/2184-8661.2026.v6i1.507