The Internet of Things Presents: A Case Study on Ensuring Legitimacy for Building Data Supply Routes in Surveillance Capitalism

NILS S. BORCHERS[1]
University of Tübingen, Germany

Surveillance capitalists dispossess data on a massive scale to extract surplus value. While pioneers such as Google entered uncharted territory when they established their data supply routes, latecomers to surveillance capitalism, among them many born-analog firms, face the challenge of building such routes in an environment that is far more hostile to maneuvers of data dispossession. This article presents a case study of how the born-analog firm Bosch attempts to build data supply routes and transform itself into a surveillance capitalist. It contributes to existing research on how surveillance capitalists ensure legitimacy for their large-scale data dispossession. It investigates a case with less-considered characteristics—a born-analog (not born-digital) firm from Germany (not the United States) targeting consumers (not policy makers or journalists)—and, thus, adds heterogeneity to the studied cases. This study finds that Bosch employs strategies of seductive surveillance and privacy washing that aim to make the processes of data dispossession invisible.

Keywords: data dispossession, surveillance capitalism, data supply routes, Internet of Things, legitimacy, privacy washing

Data supply routes constitute a central block in the infrastructure of surveillance capitalism (Zuboff, 2019). For their business models to function smoothly, surveillance capitalists require constant flows of data on a massive scale, and it is through their data supply routes that they organize these flows. Couldry and Mejias (2019) suggested understanding digital capitalism, driven by corporate surveillance, as data colonialism. This approach helps develop an initial idea of data supply routes. In historic colonialism, we can imagine supply routes as (1) the taking of valuable resources (e.g., rubber, ivory, or gold) in the colonized territory, usually from the local population and by force, (2) the transport of these materials to the motherlands, and (3) their delivery to the warehouses of the colonizing company. We can also observe these three elements in data colonialism, where (1) data are captured at the locations of technology usage, (2)

Nils S. Borchers: nils.borchers@uni-tuebingen.de
Date submitted: 2023-06-08

[1] I would like to thank two anonymous reviewers for their valuable feedback on the initial manuscript, Hendrik Theine and Sebastian Sevignani for their patient work as guest editors, and Pauline Vogt for directing my attention to the #LikeABosch campaign.

then transported away from these locations via the infrastructure of the Internet, and (3) finally enclosed on the servers of surveillance capitalists.

As this, admittedly oversimplifying, account of data supply routes reveals, the underlying process raises serious ownership issues. Not only is data moved from one place to another, but its ownership also changes. In fact, various authors have described this process as a maneuver of data dispossession (Couldry & Mejias, 2019; Thatcher, O'Sullivan, & Mahmoudi, 2016; Zuboff, 2019), a concept that establishes a clear connection to issues of data ownership. Surveillance capitalists act as if they possess the data they collect via their supply routes. They take great liberty to copy, structure, analyze, sell, and process the data in any way they choose. Furthermore, they can even destroy the data, which is a key component of property (Redecker, 2020). Hence, data supply routes constitute the practical implementation of the abstract maneuver of data dispossession.

Compared with the pioneers of surveillance capitalism like Google/Alphabet, Facebook/Meta, and Microsoft, most born-analog companies are latecomers to the data party. However, they face increasing pressure to develop surveillance-driven business models and transform into surveillance capitalists. Consider, for example, the car industry. "Your car's data may soon be more valuable than the car itself," CNN headlined in 2017 (McFarland, 2017), and a 2021 McKinsey report on "Unlocking the full life-cycle value from connected-car data" described the many ways in which "mobility players" can generate behavioral surplus from car data, while hammering home the message that they "need to act now" if they want a piece of the pie (Bertoncello, Martens, Möller, & Schneiderbauer, 2021, para. 1). Similar assessments exist for most other industries, so born-analog firms are increasingly rushing into surveillance-driven business models.

In this article, I offer a case study of how a particular born-analog company, Bosch, has taken on the task of building data supply routes to transform itself into a surveillance capitalist. In doing so, I suggest that analyzing Bosch as an emerging surveillance capitalist helps parse the company's recent ventures. Bosch is a major German technology company that operates in many different business sectors, such as thermotechnology, burglar alarms, and automotive electronics. Although the transformation into a surveillance capitalist has a technical side (i.e., building smart objects and capturing the data they generate), this study focuses on its communicative dimension. It asks how Bosch attempts to gain legitimacy for dispossessing data while transforming itself into a surveillance capitalist, and, more specifically, how it does so among a particular stakeholder group, its customers. This is a crucial stakeholder group because Bosch's transformation is essentially based on building data supply routes to appropriate user data.

This study contributes to research on how surveillance capitalists navigate the highly controversial yet existential (for them) debate on data ownership by adding heterogeneity to the analyzed cases. Whereas the question of how surveillance capitalists actively work to create a social climate that furthers their maneuvers of data dispossession has caught some interest before (e.g., Huberman, 2021; Turow, 2021; Zuboff, 2019), I examine a case with characteristics that have attracted little to no attention—Bosch is a born-analog firm from Europe that directly addresses consumers to gain legitimacy for its data dispossession activities. In doing so, this study seeks to deepen our understanding of surveillance capitalism beyond the case of Bosch. Surveillance capitalism becomes observable in the actions of surveillance capitalists;

therefore, looking into the legitimation strategies of individual companies should yield insights into surveillance capitalism itself.

The Quest for Data in Surveillance Capitalism

Surveillance Capitalism Relies on Data Dispossession

Surveillance capitalism, according to its primal analyst, Shoshana Zuboff (2015), is a "new form of information capitalism [that] aims to predict and modify human behavior as a means to produce revenue and market control" (p. 75). Google's discovery of behavioral surplus marked the beginning of surveillance capitalism. Behavioral surplus designates the data that go beyond service improvement (Zuboff, 2019). Used to feed machine intelligence, this surplus data have immense predictive power.

The crucial point, from the perspective of this study, is that surveillance capitalists need to obtain massive amounts of data to produce powerful prediction products. Malmgren (2019) observes that "surveillance capitalists accumulate wealth by commodifying and claiming ownership of whatever passive human behaviors they can systematically observe" (p. 44). This maneuver of data dispossession draws on a profound power asymmetry between the user and the surveillance capitalist, which works in favor of the latter. As Sadowski (2019) emphasizes, "data is taken with little regard for consent and compensation" (p. 1). Data dispossession is only meaningful for surveillance capitalists if implemented on a mass scale because "data about one individual's actions or properties at one moment needs to be combined with data about other actions, moments, and properties to generate valuable relations between data points" (Couldry & Mejias, 2019, p. 338). Thus, it facilitates data accumulation processes (Fuchs, 2013; Sadowski, 2019).

How to Ensure Legitimacy for Building Data Supply Routes

To dispossess data, surveillance capitalists build data supply routes. For Zuboff (2019), these routes constitute one of the central mechanisms of surveillance capitalism. Historically, Google Search has been heralded as the first such route. As Zuboff (2019) notes, "the discovery of behavioral surplus in 2001–2002 meant that Google Search would be the first Google 'service' to be re-crafted as a supply route" (p. 130). Re-crafting a service as a supply route means designing it to capture as much data as possible by default. For Google Search, this implies capturing data beyond the search queries on the Google.com website. In many cases, Zuboff (2019) argues, products merely serve as a pretext for supply routes: "Goods and services are merely surveillance-bound supply routes. It's not the car; it's the behavioral data from driving the car. It's not the map; it's the behavioral data from interacting with the map" (p. 131).

Zuboff (2019) identifies two key movements in managing data supply routes. The first is the continuous search for new supply routes. Here, most surveillance capitalists operate on the principle of trial and error. If a new route does not prove productive, it is either modified until it delivers a minimum level of productivity or it is closed (remember Google Glass?). Once surveillance capitalists have identified a productive route, they go to great lengths to secure it. This is the second movement. To illustrate how surveillance capitalists secure their supply routes, Zuboff (2019) discusses Google's "fortification strategy" (pp. 121–127). This strategy consists of four elements. All four elements target policy stakeholders, and the first three do so in a direct manner. First, Google promises to help win and defend political offices by putting its microtargeting skills at the service of political candidates and parties. Second, through its lobbying activities, Google promotes the idea that its corporate interests serve the public interest. Third, it encourages staff migration from Google to state administration and vice versa. Fourth, Google seeks to win influence over the academic debate in relevant research fields and civil society advocacy. It does so to influence policy stakeholders indirectly via public opinion and policy formation.

By targeting policy stakeholders, Google's fortification strategy aims to secure a friendly regulatory environment for the firm's surveillance-based operations. In essence, these activities boil down to ensuring Google's legitimacy. If politics considers Google's operations legitimate, this will motivate the adoption of regulations that do not restrain Google's revenue model. However, this perspective on legitimacy is somewhat abridging because Zuboff (2019) ties legitimacy strictly to only one stakeholder group, policy stakeholders. The few other stakeholder groups she considers serve merely instrumental purposes in influencing policymaking. In contrast, corporate communication research offers a broader perspective on legitimacy (e.g., Stokes, 2018). It suggests understanding legitimacy as the license to operate that society grants to a corporation. Society—in this understanding, the sum of all stakeholder groups—does so if it considers the corporation's purpose and actions to be righteous and acceptable. From this perspective, legitimacy depends on more stakeholder groups than just policy makers. For example, if consumers feel that Google's surveillance-driven business model is unethical, this could threaten Google's license to operate and, in extreme cases, lead to consumer boycotts of the firm.

This broader perspective indicates that to understand how surveillance capitalists ensure legitimacy for dispossessing data, it is worthwhile to also consider activities that target other stakeholder groups. In his investigation into the voice intelligence industry, Turow (2021) examined the role that journalists, often targeted by surveillance capitalists' media relations departments, play in the diffusion of voice-controlled appliances. Turow (2021) concluded that surveillance capitalists

> have encouraged a media depiction of voice tech that wavers confusingly between cheerleading about convenience, efficiency, and entertainment, on the one hand, and assurances by the firms involved that the surveillance isn't as bad as some claim, on the other. (p. 187)

Meanwhile, Boatwright and White (2020) offered an analysis of Facebook's online newsroom posts. The authors found that although Facebook addresses topics such as data use, transparency, and privacy, the company claims to collect data merely to improve its service. At the same time, Facebook's communication is purposefully ambiguous in that it avoids clear statements about how the company collects and uses data. Less is known, however, about how surveillance capitalists directly target consumers without taking the journalism detour.

The Internet of Things Opens New Possibilities for Born-Analog Latecomers

For the pioneers of surveillance capitalism, building data supply routes was comparably easy. As born-digital companies, these pioneers offered products whose technology possessed the inherent ability to capture data. They also entered uncharted territory and thus had to compete with only the few competitors who had ventured this far. These early activities of the new top dogs ultimately meant that for latecomers to surveillance-driven business models—such as most born-analog firms—there was little space left to construct their own data supply routes.

In this environment, The Internet of Things (IoT) promises to open unclaimed territory for born-analog firms. Equipping everyday objects such as heating systems, household electronics, and toys with sensors—that is, making "dumb" appliances "smart"—creates new possibilities to dispossess data. Critical observers have long warned against this expansion of the surveillance zone (Sadowski, 2019; Zuboff, 2019). Couldry and Mejias (2019) outline the rationale that drives the rush into IoT: "To install into every tool for human living the capacity to continuously and autonomously collect and transmit data within privately controlled systems of uncertain security" (p. 344). Data dispossession via IoT-ready devices is becoming another major manifestation of "liquid surveillance." Lyon (2010) coined this term to capture how contemporary surveillance "does not keep its shape; it morphs and mutates" (p. 330). Through "smartifying" everyday objects, surveillance capitalists promise improved functionality, yet at the same time transform these objects into surveillance devices that create new data flows, which they then harvest.

Conveniently for many born-analog firms, the now to be data-colonized territory connects to their original business fields such as heating systems, household electronics, and toys. However, as born-analog firms that market born-analog appliances, they need to explain why consumers should suddenly use, for example, a smart refrigerator after having used a dumb refrigerator all their lives. More so, they need to do this in a climate of a general unwillingness to grant companies access to personal information (Turow, Lelkes, Draper, & Waldman, 2023), and they need to do this, while there are many dumb alternatives available on the market that consumers could choose. Therefore, I argue that in adopting surveillance-driven business models, born-analog firms must pay special attention to consumers to secure their license to operate. Following this rationale, I pose the following research question: *How do born-analog companies attempt to ensure legitimacy among consumers to build data supply routes?*

Methods

This article offers a case study of the German technology company Bosch. I argue that the case of Bosch is instructive because it provides insights into a surveillance capitalist that exhibits less studied characteristics. In particular, previous research on surveillance capitalists' struggles for legitimacy has directed its focus (1) on the more spectacular cases of digital pioneers such as Google and Facebook (Boatwright & White, 2020; Lischka, 2019; Zuboff, 2019), but has overlooked born-analog companies; (2) on companies based in the United States (Dror, 2015; Huberman, 2021; Turow, 2021), but has largely neglected the activities of companies from other regions of the world such as Europe; (3) on corporate activities targeting policy stakeholders (Lischka, 2019; Zuboff, 2019), journalists (Boatwright & White, 2020; Turow, 2021), and investors (Dror, 2015), but has placed little emphasis on the strategic communication activities that directly address consumers as another important stakeholder group. As a born-analog company from Europe whose legitimation strategy focuses on consumers, Bosch combines these three understudied characteristics.

Case Description

Bosch is an engineering and technology company with headquarters in Gerlingen, Germany. It was founded by Robert Bosch in Stuttgart in 1886. It has steadily grown in importance since then. Today, with 420,000 employees worldwide and a sales revenue of 88.4 billion Euros in 2022 (Bosch, n.d.a), Bosch ranks among the largest European companies. Moreover, it holds a place among the 10 most innovative companies in Europe (European Patent Office, 2022).

Bosch organizes its activities into four business sectors: mobility solutions, industrial technology, consumer goods, and energy and building technology. All the four sectors have witnessed a massive intake of data-driven technologies in recent years. IoT plays a key role in this process. In the subsection "Strategy and Innovation" of their 2016 business report, Bosch shared its plan to transform into an IoT company:

> Our goal is to become one of the world's leading IoT companies. Coming from a classic product-manufacturing background, the strategy we pursue here is one of significantly enhancing our expertise in software and connectivity. We will use connectivity to further develop our traditional business. In addition, entirely new business opportunities are opening up. (Bosch, 2017, p. 30)

Only five years later, in its 2021 business report, the rhetoric had changed markedly. Here, Bosch announced much more confidently, "As a leading IoT provider, Bosch offers innovative solutions for smart homes, Industry 4.0, and connected mobility" (Bosch, 2022, p. 5). Increasingly, Bosch is striving to combine IoT with artificial intelligence: "The Bosch Group's strategic objective is to facilitate connected living with products and solutions that either contain artificial intelligence (AI) or have been developed or manufactured with its help" (Bosch, 2022, p. 5). These documents bear witness to Bosch's rapid transformation into a surveillance capitalist.

Bosch communicates its transformation through the #LikeABosch campaign. The hashtag #LikeABosch is an adaption of the Internet meme #LikeABoss that signifies mastery in performing activities. The first video of the campaign, managed by the renowned German advertising agency Jung von Matt NEXT ALSTER, aired on YouTube in 2019. Shorter versions of some of the following campaign spots were also later aired as TV commercials in countries worldwide, such as the United States, the Netherlands, and Indonesia. By early 2024, the campaign videos had collected more than 150 million views on YouTube alone, making it a true viral success. The advertising community welcomed this campaign euphorically and awarded it a golden Effie in the category "Transformation B2C" at the 2020 German Effie Awards.

At the center of the first-generation spots is Shawn Ryan, a 30-something, White, nerdish bachelor living in a U.S.-style stereotypical suburb who has equipped almost all areas of his life with Bosch smart technology. In later videos, additional protagonists enter the scene, culminating in the 2023 "sensor-tech" spot that brings together all relevant characters. The campaign music is an important stylistic device. It is a lyrically adjusted remake of the rap song "Like a Boss" by The Lonely Island. Characteristically, the campaign slogan "Like a Bosch" is added to every line. To get a better feel for the campaign, I invite you to watch the campaign's first spot, *The Internet of Things presents – #LikeABosch* (Bosch Global, 2019).

Data Collection and Analysis

This case study consists of two parts. The first part is an analysis of the #LikeABosch campaign. To create the corpus for my analysis, I followed formal criteria to identify all videos that were uploaded to YouTube by a general Bosch account and used the hashtag #LikeABosch or the "Shawn presents" signifier. In addition, I considered information richness (Patton, 2002, p. 230): Formally, I included only spots with a minimum length of 30 seconds; about content, I included only spots that followed the narrative of the campaign, which led to the exclusion of, for example, making of videos, videos presenting cover versions of the campaign song, and spots for staff recruitment. The final corpus for analyzing the campaign consisted of 22 videos published on YouTube by official Bosch channels between 2019 and 2024.[2] To identify the central themes of the campaign and explore how these themes connect to each other, I analyzed the videos using qualitative content analysis. I used the subsumption strategy described by Schreier (2012). This inductive strategy involved a close reading of the material, during which I created initial codes for every new aspect identified in the data. I then sorted the initial codes by compiling them into thematic groups and introducing hierarchy levels. I repeated these steps to develop the final coding frame. To include both the visual and the textual levels, I added video files and video transcripts to MaxQDA, and then employed the coding functions to develop the coding frame and conduct the coding sessions.

For the second part, I investigated supplementary data to contextualize the findings from the qualitative content analysis. These data came from a heterogeneous set of publicly available sources and included, among others, websites, presentations at trade shows, annual reports, and manuals for smart Bosch devices. In analyzing these data, I adopted a deductive approach and purposefully searched for mentions of data, IoT, etc. I included these documents in the analysis to contrast the images of the #LikeABosch campaign with materials that serve other functions, such as sharing legally binding information, explaining functionalities, and engaging with other stakeholder groups.

Findings

Central Themes in the #LikeABosch Clips

In my analysis of the #LikeABosch campaign, I identified five central themes: convenience (addressed in 17 of the 22 spots), sustainability (11/22), efficiency (8/22), status (7/22), and security and safety (6/22).

[2] See supplementary material here for a full list of videos analyzed:
https://www.dropbox.com/scl/fi/byiestdy8mahh4rba4bmd/Supplementary-Material-for-the-article-The-Internet-of-Things-Presents-by-Nils-S.-Borchers.pdf?rlkey=a8l9paerg1dibortbnxna816m&st=sb16emhg&dl=0

Convenience

In the imaginary of the campaign, convenience means, first and foremost, that smart devices relieve their owners of everyday tasks. Robot vacuums clean floors and robot mowers mow lawns, all without the intervention of their owners. For instance, the spot *The Internet of Things presents – #LikeABosch* (Bosch Global, 2019) shows the main character, Shawn, performatively dropping eggshells onto the kitchen floor, just so that his vacuum cleaner immediately mops up the shells ("I let it drop—Clean it up" [Bosch Global, 2019, 0:23]). The clips establish two lines of implications. The first line leads from convenience to ease in everyday life and further to time saving. The owners of Bosch smart appliances do not have to take care of the household chores themselves, but the appliances look after these chores. This not only saves the displeasure but also the time of executing the tasks. Essentially, using Bosch smart appliances earns their users time prosperity and thus helps cure one of the great shortages of modern (middle-class) civilization. The second line highlights the problem-solving qualities of Bosch devices. In another spot, *Shawn presents: Mercedes-Benz and Bosch Smart Home* (Bosch Smart Home, 2021), Shawn rushes out of his house and into his car. "Pressure in the morning?" he asks, addressing the viewer, "Seems familiar." After driving down the road for a while, Shawn again addresses the viewer: "Having to be on time for work? And then you wonder . . .," and, turning to his car, he says, "Hey Mercedes!" "How can I help you?" the voice control of the car replies. "Did I forget to shut the lights off at home?" "Let me check it out for you. The lights in the living room are still turned on. Do you want me to turn them off?" "Yes, ma'am!" "My pleasure, I'll turn off the lights in the living room." (Bosch Smart Home, 2021, 0:06). As this dialogue illustrates, Bosch's smart appliances make it easier to navigate everyday situations. Instead of having to drive back to check the lights, smart technology solves the problem on the fly. The greater benefit of this problem-solving ability lies in increased sovereignty in navigating everyday life. While in the Shawn episode, this sovereignty concerns his professional appearance—Shawn will be on time for work—in the spot *Bosch presents: High-tech #LikeABosch* (Bosch Global, 2022), it affects being a good parent. Here, the self-named "high-tech mom" playfully demonstrates how she masters the challenges of a working mother's life using Bosch appliances. Even while at work (again, on time, thanks to the Bosch navigation system), she uses Bosch devices to treat her cat ("I watch my kitchen—Hungry kitten" [Bosch Global, 2022, 0:48]) and air the room in which her son is training ("Such bad air?—I take care" [Bosch Global, 2022, 0:51]). By demonstrating her mastery of using smart technology to organize the life of her family, she simultaneously rebuts her son's accusation of being "so old school" because she allows him only "one hour of gaming a day" (Bosch Global, 2022, 0:04).

Sustainability

In the #LikeABosch campaign, sustainability refers to ecological concerns and, most prominently, to global warming. The theme surfaces in many of the spots, yet there is one spot, *Bosch presents – Live sustainable #LikeABosch* (Bosch Global, 2021), that negotiates sustainability exclusively. In this spot, Shawn meets Shawna, a girl in late childhood during a meeting at the Bosch headquarters in Gerlingen. Volkmar Denner, the CEO of Bosch and the third person in the room, reveals to Shawn that he will work with Shawna from now on ("Look Shawn, our goal is for all Bosch locations worldwide to become CO_2 neutral. And that's why we thought we should team you up with, well, someone who truly represents the future" [Bosch Global, 2021, 0:08]). Shawna then lists several measures that humanity should take to live more sustainably, which basically consist of using Bosch smart technology ("Can do so much, that's a fact. E-Bikes, heat pumps, washers, tools. Basic stuff you learn in school" [Bosch Global, 2021, 1:25]). Meanwhile, Shawn belittles her ("Bring it on, little one" [Bosch Global, 2021, 0:32]). However, when Shawna calls on Shawn to support her cause ("Stop the battle, let's unite! Carbon-neutral, that's how we fight" [Bosch Global, 2021, 1:18]), he willingly agrees. This spot connects sustainability tightly with the climate crisis and positions Bosch technology as the answer to meeting the crisis, not least in rhyming "climate crisis" with "smart devices" (Bosch Global, 2021, 1:29). This spot even suggests that consumers have the power to stop global warming if they would only make responsible choices ("Every little choice can make a change" [Bosch Global, 2021, 1:35]).

Efficiency

The theme of efficiency refers to the smarter use of resources made possible by Bosch smart devices. It closely connects to sustainability. This connection is not surprising because the efficient use of resources helps reduce the pressure on ecosystems. The spot *Whatever you drive, drive #LikeABosch* (Bosch Global, 2020a), which addresses electric mobility, even sets efficiency in direct relation to sustainability ("Top condition—Low emission (. . .)—Cause it drives—So many miles" [Bosch Global, 2020a, 0:19]). However, the efficiency theme is more complex. Another spot, *Shawn presents–Smart Home Climate #LikeABosch* (Bosch Smart Home, 2020a), starts with a lecture by Shawn:

> Do you know how much of your home's energy goes into heating? Alone in the Western countries it's more than two thirds. Which means: intelligent heating not only protects the environment. It saves you money. You can reduce your heating consumption by up to 30 percent. (Bosch Smart Home, 2020a, 0:06)

Shawn then presents the features of the Bosch smart heating system he has installed in his home ("Remote control allows me to actively save energy. I switch off the heating when not needed" [Bosch Smart Home, 2020a, 0:48]). Efficiency also emerges in the presentation of how industrial production benefits from Bosch smart technology. In a respective spot, *The Internet of Things presents – Manufacture #LikeABosch* (Bosch Global, 2020b), Shawn highlights how technology allows to avoid downtime in production processes ("Flexible line—To make it mine—No downtime—That's worth a rhyme" [Bosch Global, 2020b, 0:35]). The spot then uses Bosch IoT technology to link the avoidance of downtime to efficiency; even more so, it identifies increasing efficiency as Bosch's mission ("Control the tech—Phone check—Go 5G—IoT—So efficient—That's our mission" [Bosch Global, 2020b, 0:51]).

Status

By using Bosch's smart appliances, its users increase their social status. The campaign translates this status into the approval or even admiration that peers give to Bosch users. In the sustainability spot (Bosch Global, 2021), Shawna points out how her peer group appreciates that she is using e-mobility ("Charging E—Electric drives—My crew likes"). Other spots also show how Shawn uses the Bosch technology to impress others. He impresses his neighbor, Sean, with his robotic mower ("I mow the lawn—Impressing Sean" [Bosch Global, 2019, 0:17]). He also impresses a group of decidedly casual people in their early 20s, sitting in a vintage convertible, with his technology-packed Mercedes ("Get in the car—Superstar—They're watching me—IoT" [Bosch Global, 2019, 0:30]). In general, Bosch devices are depicted as "cool," and this quality rubs off on their users ("Look, that's cool, too: voice control! 'Alexa, set scenario: perfect evening!' All you need is a few devices and the wish to be smart" [Bosch Smart Home, 2020a, 1:08]).

Security and Safety

Security and safety revolves around the promise that Bosch smart appliances reduce the risk of their users harming themselves or others. There are two subthemes. The first subtheme, anti-burglary protection, appears in only one spot, *Shawn presents: Sicher Leben #LikeABosch* (Bosch Smart Home, 2020b), yet this spot focuses exclusively on this topic. Here, Shawn demonstrates how Bosch technology helps secure his home from burglars ("But what can we do to feel safer? The answer is: Bosch Smart Home" [Bosch Smart Home, 2020b, 0:10]). The second subtheme, traffic safety, appears more frequently. A recurring motif includes vehicles (cars and bicycles) that stop autonomously because a person (or an alpaca) crosses their paths unexpectedly. Bosch technology also helps its users keep their balance on motorcycles or park their cars without denting them. These episodes fall into a general narrative thread that portrays Bosch technology as a reliable and effective assistant to its human users.

Control It #LikeABoss

Cutting through these five themes is the campaign's title, #LikeABosch. It refers to mastery in performing activities, and this mastery is imagined as smart tech-afforded, for example, when the protagonists use Bosch devices to feed the cat at home (*convenience*) or manage resources (*efficiency*). In the bigger picture, the campaign shows individuals who are in control of the tasks they need to handle, from carrying out their daily chores to fighting global warming. However, this is only the endpoint of a little control cascade, beginning with control over the Bosch devices. By controlling the technology ("Control the tech" [Bosch Global, 2020b, 0:51], see *efficiency* for full quote), users have the power to control their environments ("Control your home from your car with voice control" [Bosch Smart Home, 2021, 1:29]), and this puts them into control of tasks ("Cut precise—Lawn so nice—What a flex—Smartwatch tracks—See me roll—In control" [Bosch Global, 2023, 0:14]). Notably, controlling technology, the starting point of the cascade, is presented as dead easy. The devices are easy to install, as Shawn explains: "Installation of Bosch smart home was easy. It only took me about half an hour, and I'm definitely not the most tech-savvy person around" (Bosch Smart Home, 2020b, 1:27); and the devices are easy to use, be it via voice control (see the Mercedes episode above) or an app installed on the smartphone ("I tap the phone—Coffee's on" [Bosch Global, 2019, 0:13]). The control idea is where the origin of the slogan, #LikeABoss, shines through: the users are the bosses of the Bosch devices, the devices are their assistants. However, as I will explain in the following, what remains invisible is that the devices also serve another master.

Data Ownership as a Nontheme

In the communication accompanying the campaign, Markus Heyn and Mike Mansuetti, both high-ranking Bosch managers, addressed the users' control over what happens to their collected data. During the 2019 CES in Las Vegas, they announced:

> Making responsible use of people's personal data is a top priority for Bosch. That includes being open about what information we store and process, and what we use it for. When it comes to all of our smart solutions, you as the user, have full transparency and control over the data they collect—if you don't want it leaving your premises, it won't. (Heyn & Mansuetti, 2019, para. 50)

In this statement, the two Bosch officials promise consumers transparency and data sovereignty. However, this promise is in stark contrast with the absence of data ownership in the #LikeABosch campaign. In fact, "data" is mentioned in only one instance. In the spot *The Internet of Things presents – Manufacture #LikeABosch*, which addresses industrial production, a data cloud appears, while the campaign song states: "Data cloud—Makes me proud—Together we—Save energy—IoT" (Bosch Global, 2020b, 1:09). The visual representation of the data cloud consists of small white clouds that form a face against a blue sky. The whole setting creates a peaceful impression. It is also striking how the text first rhymes "data cloud" with "makes me proud" and then establishes a direct link to energy saving and IoT. The attempt to frame the data cloud positively is obvious. At the same time, the scene remains suspiciously silent about the fact that the data stored in the cloud must originate from somewhere and that their generation includes maneuvers of data dispossession. It also overlooks the massive energy consumption of cloud servers, big data processing, and AI applications (Brevini, 2020).

Building an Infrastructure for Dispossessing Data

Bosch's interest in data dispossession is evident in its Terms of Services (ToS). Consider, for an instructive example, the Bosch robot vacuum from the Roxxter BCR1 series. In the section entitled "Data protection information" (Bosch, n.d.c, p. 91), the manual lists the data that Roxxter BCR1 transmits to Bosch's Home Connect Server for the initial registration. These data include the unique appliance identification, the security certificate of the wireless networking communication module, the current software and hardware versions, and the status of any previous restoration of the factory settings. These data have a clear connection to service improvements rather than to behavioral surplus. However, the crux is that the "Notes" subsection to the "Data protection information" section specifies that the use of Home Connect functions requires the Home Connect application, which has its own privacy notice. The Home Connect app is provided by the Residential IoT Services GmbH, a company owned by Bosch. The FAQs section on the app's website provides an initial idea of data dispossession. Here, the answer to the question "Can I prevent my appliance from sending any data?" is that "certain functions are reliant on the status, that the appliance is connected with the server. But of course you are free to decide for or against using additional functions that the networked appliances can offer you" (Bosch, n.d.b). When looking more closely at the app's "privacy notice" (Home Connect Plus, n.d.), one gets a more specific overview of the data that are first transmitted from device to app and then transported to the Home Connect server via the data supply routes. Here, the reader learns that (Home Connect Plus, n.d.):

- The app registers information on connected devices, such as the robot vacuum. This information includes, among others, the stable ID of the connected device and its status, tagged with a time stamp (para.11).

- The app shares collected data with external service providers for "tasks such as customer surveys, programming, data hosting, sales and marketing, contract management, and technical operations" (para. 15).
- Some functions for controlling the connected devices via the app require data on the device location, which the app determines via the Google Maps Geocoding API (para. 20).
- The app interacts with the "Adjust" analytics service "to analyze user behavior and thus optimize our advertising campaigns." To do so, the app processes wide-reaching information, such as IP addresses, MAC addresses, user agents (i.e., country, language, settings, operating system), information about the device and the user's web activity, app and event tokens, and interactions on other companies' ad networks. The privacy notice further states that Adjust "uses your device identifiers to display relevant ads to you on your mobile device on other companies' ad networks" and explains that the captured data may be shared with third companies (para. 21).
- The app uses an advertising identifier. "We use the identification numbers to provide you with personalised advertising and to analyse your usage." Users can limit the use of the advertising identifier and thus the variety of captured data, but "if you limit use of the identification number, you may not be able to use all the functions of our App" (para. 19).

The data that Bosch captures thus widely exceed the demands of service improvement. While users can opt out of passing on some of the data, the app's privacy notice, like the robot vacuum's data protection information, evokes a rather unspecific threat scenario, which claims that if curtailed of their connectivity (i.e., data sharing), the Bosch devices will lose their smartness and thus not deliver the benefits the #LikeABosch campaign portrayed.

Another example of Bosch's hunger for data, besides ToS, is the diversity of data that the smart devices can collect. For instance, the newest generation of Roxxter vacuum robots possesses cameras and is thus able to collect visual data. Bosch frames this feature in terms of added functionality when explaining that it allows users to see particularly dirty areas in the home or monitor from afar whether all windows are closed (Bosch, n.d.d). Bosch also praises the devices' compatibility with voice control systems, such as Amazon Alexa (Bosch, n.d.d), which indicates the willingness to capture voice data (Turow, 2021).

In the logic of surveillance capitalism, dispossessing data via supply routes and storing it on the surveillance capitalist's servers is only one step in the value chain. Accordingly, Bosch is building a data processing infrastructure, which the company feeds with the dispossessed data. Bosch's annual report for 2021 gives an idea of how massive this infrastructure for storing, structuring, and analyzing data have become. Bosch (2022) elaborates:

> The Bosch IoT Suite connects different devices to the relevant IT infrastructure (backend) solutions and collects the data transmitted by these devices. The Bosch hybrid cloud acts as a universal platform for securely processing and storing data. The RED Lake (Robert Bosch Enterprise Data Lake) gives the data structure and makes it accessible in the company. The AI platform (under construction) analyzes the data, generates knowledge, and determines what action to take. The aim is to gradually grow the number of customers

> and of products that are in fact digitally connected, to intensify the company's data focus, and to advance the maturity of the AI platform. (p. 44)

Bosch's emerging data processing infrastructure presented here stands in marked contrast to the absence of data in the #LikeABosch campaign. Setting up such an infrastructure only makes sense if it is fed with massive amounts of data.

Building Legitimacy Through Seductive Surveillance and Privacy Washing

The #LikeABosch campaign is the heart of Bosch's communication activities accompanying the company's endeavor to ensure legitimacy for establishing a surveillance-ready infrastructure. To spur consumers' adoption of Bosch's smart devices, the campaign presents these devices as the key to a new, smart lifestyle that brings many benefits. When using Bosch smart appliances, consumers enjoy a life that is more convenient, sustainable, efficient, prestigious, safe, and secure.

The five themes the campaign builds on can hardly be considered innovative. As Lyon (2002) points out, surveillance is an ambiguous process because it is both a threat and a promise. Lyon recalls that "much everyday convenience, efficiency, and security depends on surveillance" (p. 243). The same is true for the connection between the early adoption of consumer technology and high social status (Stebbins, 2009) and the techno-solutionist imaginary that smart technology will stop global warming (Brevini, 2020). The campaign thus attempts to gain resonance by evoking themes that are firmly anchored in public discourse and are therefore familiar to consumers.

From Seductive Surveillance to Habituation

While the campaign emphasizes the benefits of using Bosch smart technology, it blanks out questions of data and its dispossession. At the level of the campaign, we can thus see an agenda-setting/agenda-cutting dynamic unfold (Buchmeier, 2020): Bosch seeks to legitimize its transformation into a surveillance capitalist by shifting the debate away from questions of data ownership. Troullinou (2017) suggested analyzing strategies that deploy such dynamics as seductive surveillance. Seductive surveillance implies that "ICTs are presented as tools in the hands of the users to enhance their participation to decision making process [sic!] at a societal level and their everyday life at an individual level, eschewing the risks of their use" (Troullinou, 2017, p. 64). It is easy to identify this pattern in the #LikeABosch campaign. The Bosch-afforded smart lifestyle includes many such promises of enhanced participation, such as when Bosch users navigate their everyday lives with great sovereignty (individual level) or stop climate change (societal level). Another core aspect of seductive surveillance can also be observed in the Bosch campaign. Troullinou (2017) points out that seductive surveillance runs on the impression that the interests of corporations and consumers align. Such an alignment of interests becomes most explicit in the sustainability clip discussed above (Bosch Global, 2021; see theme "Sustainability"). Here, Bosch CEO Denner announces the goal "to become CO_2-neutral," while Shawna, and later Shawn, present smart technology as the solution to consumers' wish to act sustainably. Yet, the self-efficacy users gain comes at the price of a comprehensive surveillance regime that allows Bosch to dispossess user data.

Seducing consumers into trying out Bosch smart technology is only the first step in setting up data supply routes. The next step is to consolidate the use of this technology so that Bosch can permanently dispossess the data. In his analysis of the voice intelligence industry, Turow (2021) identified this step as habituation. Once consumers get used to the ease that these devices bring to their lives, they will find it hard to do without them. In this phase, surveillance capitalists can increase the scope of their data dispossession without having to fear fierce resistance. Given that it operates in markets where dumb alternatives are easily available to consumers, entering this phase is crucial for Bosch. Various observers have pointed out that the Terms of Service (ToS) play a vital role in the process of data dispossession (e.g., Kienscherf, 2022; Thatcher et al., 2016). Surveillance capitalists have previously used ToS to increase the scope of their data dispossession, even retroactively, and Bosch might be inclined to use the same strategy once consumers have reached the stage of habituation. In addition, my analysis showed that Bosch is already using the ToS to create a threat scenario designed to discourage users from opting out of data sharing. The ToS claim that Bosch's smart devices will lose some of their functionalities and, ultimately, their smartness when limiting data sharing. In doing so, the ToS remain strategically vague. Rather than specifying the functions that will be affected by deactivating data sharing, they vaguely speak of "certain functions." The tradeoff that the ToS present to users is thus one between functionality and data sovereignty.

Privacy Washing

In moving this analysis beyond the level of the #LikeABosch campaign, we can see that Bosch engages in practices of privacy washing. Privacy washing includes making claims about the processing of personal data that obscure the scope of the actual processing (Aïvodji et al., 2021). As such, privacy washing is a useful concept to pin down and critically scrutinize surveillance capitalists' communicative activities. To increase its applicability, I suggest broadening privacy washing to also include (1) claims about data capture (in addition to data processing) and (2) blank spaces in strategic communication (in addition to explicit claims), that is, when data-related activities are conspicuously absent from the interactions. As my analysis demonstrates, Bosch avoids making statements about either data dispossession or data processing. In fact, the campaign addresses data collection in only one instance. This gives the impression that Bosch's smart technology functions without an underlying data infrastructure. Thus, there is a stark contrast between the virtual absence of the data theme in the campaign and Bosch's assertion of users' data sovereignty on one hand and the threat scenario of function failure that Bosch put into the ToS to secure its ability to dispossess user data on the other. Moreover, the campaign communications omit that Bosch is building a massive infrastructure for processing dispossessed data. This omission should be set against a backdrop of consumer unease about data usage in the context of smart home devices. Survey data from Germany reveal that consumers' top three concerns about smart home technology are all data-related: fear of hacker attacks (47% of consumers), fear of data misuse (37%), and fear of privacy violations (29%; Bitkom, 2022, p. 16).

In an insightful article, Draper and Turow (2019) identified what they call the "corporate cultivation of digital resignation," that is, "the condition produced when people desire to control the information digital entities have about them but feel unable to do so" (p. 1824). According to the authors, the corporate cultivation of such resignation is a large-scale strategy that corporations use to discourage resistance against their surveillance-driven business models. In essence, such resistance would turn against the practices of data dispossession and, consequently, the legitimacy of current data ownership models. Privacy washing can be categorized as a practice that fits into the larger strategy of cultivating digital resignation, which, again, serves the purpose of fortifying data supply routes.

Organizing Data Ownership

Although strategies of seductive surveillance and privacy washing aim to create a competitive advantage for the company, I argue that there is more at stake. Surveillance capitalism could only unfold because (Western) societies tolerated the establishment of ownership regimes that rest on carting data off to the enclosed servers of surveillance capitalists in a colonialist manner. In contrast, models of organizing data ownership in a collective manner, such as data-owning democracy (Fischli, 2024) or digital socialism (Muldoon, 2022), pose a threat to surveillance capitalism. By denying surveillance capitalists exclusive ownership of data, they put data at the service of the common good rather than individual profit. Bosch's approach of picturing a world in which the products of a private surveillance-capitalistic enterprise solve acute problems such as climate change and time poverty—problems that society has failed to solve thus far—ultimately aims to generate legitimacy for surveillance capitalism, and its data-dependent business models, as a superior organizational structure for tackling large-scale problems.

Conclusion

In this article, I asked how born-analog companies attempt to ensure legitimacy among consumers to build data supply routes. I examined the case of Bosch and its #LikeABosch campaign. My analysis demonstrated how Bosch is communicatively flanking the re-crafting of its products as data supply routes—just like Google did with search (Zuboff, 2019, p. 130). I suggested applying the concepts of seductive surveillance (Troullinou, 2017) and privacy washing (Aïvodji et al., 2021) to theorize the gap between the data-free world that the #LikeABosch campaign pictures and the stark reality of data dispossession. According to Zuboff (2019, p. 131), in surveillance capitalism, products merely serve as a pretext for data supply routes. While it is not clear at this point if and how Bosch plans to reap behavioral surplus, the company operates under ToS agreements that allow for a massive capture of behavioral surplus. It also puts an infrastructure in place that allows for data dispossession on a massive scale. I interpreted these activities as evidence for the determination with which Bosch is embracing a surveillance-driven business model.

This study contributes to research interested in the communicative activities that surveillance capitalists unfold to build and secure their data supply routes (e.g., Boatwright & White, 2020; Lischka, 2019; Zuboff, 2019). It expands the body of research by examining the case of a firm that is born-analog, originates from Europe, and focuses its activities directly on consumers. These three features have received little attention so far. Nevertheless, it should be noted that I was only able to draw on publicly available documents to reconstruct my case. Hence, I cannot say for sure whether my analysis is complete. Furthermore, the approach of focusing on a single company does not allow for broader generalizations. Rather, it adds a particular detail to the bigger picture of surveillance capitalists' strategies to fortify their data supply routes. We need additional research to make this picture more complete. In particular, I encourage researchers to identify further heterogeneity criteria to ensure that research can overcome its current focus on born-digital firms in the United States. Analyses of how companies with other characteristics confront the challenges of re-crafting their products as data supply routes will facilitate a more nuanced understanding of surveillance capitalists' strategies to legitimize their maneuvers of data dispossession. This understanding will also help inform strategies on how to tackle these legitimation strategies, with the goal of building support for alternative forms of organizing data ownership.

References

Aïvodji, U., Castets-Renard, C., Cofone, I., Gambs, S., Marcoux, A. M., & Martin, D. (2021). *Privacy and AI ethics: Understanding the convergences and tensions for the responsible development of machine learning*. Retrieved from https://sebastiengambs.openum.ca/files/sites/82/2021/11/OPC_final.pdf

Bertoncello, M., Martens, C., Möller, T., & Schneiderbauer, T. (2021). *Unlocking the full life-cycle value from connected-car data*. Retrieved from https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/unlocking-the-full-life-cycle-value-from-connected-car-data

Bitkom. (2022). *Smart home 2022*. Retrieved from https://www.bitkom.org/sites/main/files/2022-09/220912_Bitkom_Smart_Home_Chartbericht_2022_final.pdf

Boatwright, B. C., & White, C. (2020). Is privacy dead? Does it matter? *The Journal of Public Interest Communications, 4*(1), 78. doi:10.32473/jpic.v4.i1.p78

Bosch. (n.d.a). *The Bosch Group at a glance*. Retrieved from https://www.bosch.de/en/our-company/bosch-group-worldwide/

Bosch. (n.d.b). *Home Connect FAQ*. Retrieved from https://www.bosch-home.in.th/en/specials/homeconnect/homeconnect-faq#/Togglebox=3931260-3935581-1/Togglebox=3931260-3935583-1/Togglebox=3931260-3935584-1/

Bosch. (n.d.c). *Instruction manual: Robot vacuum*. Retrieved from https://media3.bosch-home.com/Documents/8001055415_B.pdf

Bosch. (n.d.d). *Roxxter: Five ways vacuuming just became more fun.* Retrieved from https://www.bosch.com/stories/smart-robot-vacuum/

Bosch. (2017). *Annual report 2016*. Retrieved from https://www.annualreports.com/HostedData/AnnualReportArchive/b/bosch_2016.pdf

Bosch. (2022). *Annual report 2021*. Retrieved from https://www.annualreports.co.uk/HostedData/AnnualReportArchive/b/bosch_2021.pdf

Bosch Global. (2019, January 07). *The Internet of Things presents—#LikeABosch* [Video file]. Retrieved from https://youtu.be/v2kV6pgJxuo

Bosch Global. (2020a, February 20). *Whatever you drive, drive #LikeABosch* [Video file]. Retrieved from https://youtu.be/MkthoupAgOg

Bosch Global. (2020b, June 09). *The Internet of Things presents—Manufacture #LikeABosch* [Video file]. Retrieved from https://youtu.be/1FerootGwQc

Bosch Global. (2021, January 11). *Bosch presents—Live sustainable #LikeABosch* [Video file]. Retrieved from https://youtu.be/YfLiwpwEqtU

Bosch Global. (2022, April 1). *Bosch presents: High-tech #LikeABosch* [Video file]. Retrieved from https://youtu.be/LLRQQ2YD9dk

Bosch Global. (2023, April 1). *Bosch presents: Sensor-tech #LikeABosch* [Video file]. Retrieved from https://youtu.be/ZPZfxEf-p18

Bosch Smart Home. (2020a, February 17). *Shawn presents—Smart Home Climate #LikeABosch* [Video file]. Retrieved April 30, 2022 from https://youtu.be/mRhVUjtKuTQ

Bosch Smart Home. (2020b, February 25). *Shawn presents: Sicher Leben #LikeABosch* [Shawn presents: Secure living #LikeABosch] [Video file]. Retrieved April 29, 2022 from https://youtu.be/1JlzZHFyOwE

Bosch Smart Home. (2021, March 01). *Shawn presents: Mercedes-Benz and Bosch Smart Home* [Video file]. Retrieved April 29, 2022 from https://youtu.be/ExdQvRx1iuQ

Brevini, B. (2020). Black boxes, not green: Mythologizing artificial intelligence and omitting the environment. *Big Data & Society, 7*(2), 2053951720935141. doi:10.1177/2053951720935141

Buchmeier, Y. (2020). Towards a conceptualization and operationalization of agenda-cutting: A research agenda for a neglected media phenomenon. *Journalism Studies, 21*(14), 2007–2024. doi:10.1080/1461670X.2020.1809493

Couldry, N., & Mejias, U. A. (2019). Data colonialism: Rethinking big data’s relation to the contemporary subject. *Television & New Media, 20*(4), 336–349. doi:10.1177/1527476418796632

Draper, N. A., & Turow, J. (2019). The corporate cultivation of digital resignation. *New Media & Society, 21*(8), 1824–1839. doi:10.1177/1461444819833331

Dror, Y. (2015). “We are not here for the money”: Founders’ manifestos. *New Media & Society, 17*(4), 540–555. doi:10.1177/1461444813506974

European Patent Office. (2022). *Patent Index 2021: Applicants.* Retrieved from https://report-archive.epo.org/about-us/annual-reports-statistics/statistics/2021/statistics/applicants.html

Fischli, R. (2024). Data-owning democracy: Citizen empowerment through data ownership. *European Journal of Political Theory, 23*(2), 204–223. doi:10.1177/14748851221110316

Fuchs, C. (2013). Political economy and surveillance theory. *Critical Sociology, 39*(5), 671–687. doi:10.1177/0896920511435710

Heyn, M., & Mansuetti, M. (2019, January 7). *IoT "Like A Bosch": How we're turning our vision of a better tomorrow into reality today.* ICS 2019, Las Vegas. Retrieved from https://www.bosch-presse.de/pressportal/de/en/iot-like-a-bosch-how-were-turning-our-vision-of-a-better-tomorrow-into-reality-today-180237.html

Home Connect Plus. (n.d.). *App privacy notice and terms of use Great Britain*. Retrieved May 01, 2022 from https://www.home-connect-plus.com/gb/en/app-legal/

Huberman, J. (2021). Amazon go, surveillance capitalism, and the ideology of convenience. *Economic Anthropology, 8*(2), 337–349. doi:10.1002/sea2.12211

Kienscherf, M. (2022). Surveillance capital and post-Fordist accumulation: Towards a critical political economy of surveillance-for-profit. *Surveillance & Society, 20*(1), 18–29. doi:10.24908/ss.v20i1.14235

Lischka, J. A. (2019). Strategic communication as discursive institutional work: A critical discourse analysis of Mark Zuckerberg's legitimacy talk at the European Parliament. *International Journal of Strategic Communication, 13*(3), 197–213. doi:10.1080/1553118X.2019.1613661

Lyon, D. (2002). Everyday surveillance: Personal data and social classifications. *Information, Communication & Society, 5*(2), 242–257. doi:10.1080/13691180210130806

Lyon, D. (2010). Liquid surveillance: The contribution of Zygmunt Bauman to surveillance studies. *International Political Sociology, 4*(4), 325–338. doi:10.1111/j.1749-5687.2010.00109.x

Malmgren, E. (2019). Resisting "Big Other": What will it take to defeat surveillance capitalism? *New Labor Forum, 28*(3), 42–50. doi:10.1177/1095796019864097

McFarland, M. (2017). *Your car's data may soon be more valuable than the car itself*. Retrieved from https://money.cnn.com/2017/02/07/technology/car-data-value/index.html

Muldoon, J. (2022). *Platform socialism: How to reclaim our digital future from big tech*. London, UK: Pluto.

Patton, M. Q. (2002). *Qualitative research and evaluation methods*. Thousand Oaks, CA: Sage.

Redecker, E. von. (2020). Ownership's shadow: Neoauthoritarianism as defense of phantom possession. *Critical Times, 3*(1), 33–67. doi:10.1215/26410478-8189849

Sadowski, J. (2019). When data is capital: Datafication, accumulation, and extraction. *Big Data & Society, 6*(1). doi:10.1177/2053951718820549

Schreier, M. (2012). *Qualitative content analysis in practice*. Los Angeles, CA: Sage Publications.

Stebbins, R. A. (2009). Conspicuous consumption. In R. A. Stebbins (Ed.), *Leisure and consumption* (pp. 30–55). London, UK: Palgrave Macmillan.

Stokes, A. Q. (2018). Legitimacy (Legitimatizing). In R. L. Heath & W. Johansen (Eds.), *The international encyclopedia of strategic communication* (pp. 1–17). Hoboken, NJ: Wiley. doi:10.1002/9781119010722.iesc0100

Thatcher, J., O'Sullivan, D., & Mahmoudi, D. (2016). Data colonialism through accumulation by dispossession: New metaphors for daily data. *Environment and Planning D: Society and Space, 34*(6), 990–1006. doi:10.1177/0263775816633195

Troullinou, P. (2017). *Exploring the subjective experience of everyday surveillance: The case of smartphone devices as means of facilitating "seductive" surveillance.* The Open University. doi:10.21954/ou.ro.0000cd85

Turow, J. (2021). *The voice catchers: How marketers listen in to exploit your feelings, your privacy, and your wallet*. New Haven, CT: Yale University Press.

Turow, J., Lelkes, Y., Draper, N. A., & Waldman, A. E. (2023). *Americans can't consent to companies' use of their data*. Annenberg School for Communication, University of Pennsylvania. Retrieved from https://www.asc.upenn.edu/sites/default/files/2023-02/Americans_Can%27t_Consent.pdf

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology, 30*(1), 75–89. doi:10.1057/jit.2015.5

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. London, UK: Profile.