

University of Kentucky

UKnowledge

---

Geography Faculty Publications

Geography

---

9-2018

## Hacking Code/Space: Confounding the Code of Global Capitalism

Matthew Zook

*University of Kentucky, zook@uky.edu*

Mark Graham

*University of Oxford, UK*

Follow this and additional works at: [https://uknowledge.uky.edu/geography\\_facpub](https://uknowledge.uky.edu/geography_facpub)



Part of the [Geography Commons](#)

[Right click to open a feedback form in a new tab to let us know how this document benefits you.](#)

---

### Repository Citation

Zook, Matthew and Graham, Mark, "Hacking Code/Space: Confounding the Code of Global Capitalism" (2018). *Geography Faculty Publications*. 32.

[https://uknowledge.uky.edu/geography\\_facpub/32](https://uknowledge.uky.edu/geography_facpub/32)

This Article is brought to you for free and open access by the Geography at UKnowledge. It has been accepted for inclusion in Geography Faculty Publications by an authorized administrator of UKnowledge. For more information, please contact [UKnowledge@lsv.uky.edu](mailto:UKnowledge@lsv.uky.edu).

---

## Hacking Code/Space: Confounding the Code of Global Capitalism

Digital Object Identifier (DOI)  
<https://doi.org/10.1111/tran.12228>

### Notes/Citation Information

Published in *Transactions of the Institute of British Geographers*, v. 43, issue 3.

© 2018 The Authors

This is an open access article under the terms of the [Creative Commons Attribution-NonCommercial License](#), which permits use, distribution and reproduction in any medium, provided the original work is properly cited and is not used for commercial purposes.

# Hacking code/space: Confounding the code of global capitalism

Matthew Zook<sup>1</sup>  | Mark Graham<sup>2,3</sup> <sup>1</sup>Department of Geography, University of Kentucky, Lexington, KY, USA<sup>2</sup>Oxford Internet Institute, University of Oxford, Oxford, UK<sup>3</sup>The Alan Turing Institute, London, UK**Correspondence**

Matthew Zook

E-mail: zook@uky.edu

Information-technologies are essential for global capitalism to function at speed across scale, space and complexity. The importance of software and algorithms in the governance of these systems is reflected in the attention of scholars to the ways digital code and materiality (re)combine to create hybrid digital/material spaces of economic activity, movement and everyday life. This paper extends this work in two key ways: first by emphasising the relational aspect of these code/spaces, and second by showing how the digital algorithms of code/spaces are hackable rather than hegemonic. Using the case study of frequent flyer programmes we demonstrate how networked knowledge-sharing reshapes code/spaces to provide unintended opportunities such as low-cost travel and access to spaces normally only frequented by global elites. Although this case highlights vulnerabilities in the code of global capitalism, it is primarily only those with significant lifestyle privilege who are able to fully participate in these subversions. Moreover, while much of the value captured by “airline hackers” comes from airlines’ profit margins, the relationality of code/spaces can impact citizens and consumers not directly connected to or interested in airline travel. Ultimately, this paper demonstrates that in contrast to characterisations of omnipresence and hegemony, the information networks and algorithms of global capitalism contain moments of uneven porosity and selective hackability.

**KEYWORDS**

air travel, airlines, code/space, digital life, hacking

## 1 | INTRODUCTION

Global capitalism fundamentally relies on information technologies to quickly manage complex constellations of economic activities across space, institutions and human lives (Castells, 1996). Central to these systems are software-based algorithms that automatically handle routinised transactions and decisions to maximise capacity and minimise transit times across space. Aggregated, these digital processes comprise a powerful network of coded governance (Zuboff, 2015) channelling the flows of global capitalism in particular ways, via particular places and to the advantage of particular actors (Graham & Marvin, 2001). The code (and algorithms constructed from it)<sup>1</sup> used to structure these constraints has a seemingly hegemonic influence over the space of the global economy (Charette, 2005). When software systems fail, e.g., the stock market flash crash of 2010 or airline computer system meltdowns, entire global operations are gravely disrupted.

This is an open access article under the terms of the Creative Commons Attribution-NonCommercial License, which permits use, distribution and reproduction in any medium, provided the original work is properly cited and is not used for commercial purposes.

The information, practices and views in this article are those of the author(s) and do not necessarily reflect the opinion of the Royal Geographical Society (with IBG).

© 2018 The Authors. *Transactions of the Institute of British Geographers* published by John Wiley & Sons Ltd on behalf of Royal Geographical Society (with the Institute of British Geographers).

It is almost impossible to avoid code within modern capitalist economies as individuals' access to credit, queuing time and even admission to certain work and living spaces turn on algorithmically determined decisions (Graham, 2005). These everyday economic and social spaces are co-constituted by both the material elements of places and the design of digital code (Thrift & French, 2002). These interactions create hybrid spaces or "code/spaces" as diverse as supermarket checkout lines and airline boarding (Kitchin & Dodge, 2011).

Of particular concern to technology critics, scholars and artists has been the extent to which these code/spaces shift power from citizens to the entities that control algorithms. This paper argues, however, that while code has power, it is not law (Lessig, 1999) and the complex entanglements of material and digital spaces are rarely fixed, but continuously reconstructed. Moreover, the functional logic of these code/spaces is relational, connecting diverse sets of places, people and programmes across a global capitalist network, and thereby creating new avenues for power, profit and victimisation. Individuals who must pass through these software systems for daily activities have ways of retaining agency, not only via obscuring themselves or direct sabotage but also through transgressions that subtly rework or hack code/space to their advantage. These subversions against the control of code, however, are not universally actionable as their ability to function often depends on their exclusivity and contingency. Thus, hacking code/space helps to produce new power-geometries that impact the control centres of global capitalism but also potentially negatively affect those on the fringes of the relational network.

We use the case study of hacking airline frequent flyer programmes – using reward points gained via loopholes to travel for little cost – to demonstrate the rewriting of the code/space of global capitalism. We highlight three techniques used to subvert frequent flyer code/space – creative use of airline geographies, credit card churning and consuming for miles – and demonstrate their intricate ensconcing within global capitalism. Hacking confounds code's hegemony over the social, but this agency does not simply equate with political liberation. Rather the complexity and often playful mischief inherent to human-machine interactions competes with code, and the outcome of this resistance reverberates across global networks in unexpected and sometimes profoundly uneven ways. Hacking code/space transgresses against capitalism but the relationality of these systems and the ability for corporations to protect themselves and shift risk ensures that ill effects are much more widespread, often with inequitable impacts to peripheral people and places.

## 2 | CODE, LAW AND THE FORMATION OF SPACE

Early research on digital geographies was often rather unidirectional in focus, concerned primarily with how information use mapped onto physical locations (Hepworth, 1989; Zook, 2000) or impacted material systems via coded errors like the Y2K bug (Thrift & French, 2002). Although scholars discussed the co-constitution of materiality and cyberspace (Graham, 1998; Hillis, 1998; Kitchin, 1998), the project to counter the "relative invisibility" of information (Hillis, 1998, p. 543) remained a key focus. In part, this emphasis reflected information technology at the time, when phones were for voice and computers sat on desktops rather than in pockets. As smartphones and geolocation applications became more prevalent, simultaneous interaction between the material and the digital layers of places became the norm for many individuals. These new hybrid spaces – the processes by which they come into being, the reciprocity between the material and the digital, and the factors that influence them – represent a burgeoning field of scholarship envisioned in three key ways.

First, echoing the unidirectional focus of the earliest work on digital geographies is a vision in which the digital dominates everyday life. Mitchell perhaps first expressed this with his argument that "out there on the electronic frontier, code is the law" (1996, p. 111). Others such as Reidenberg built on this argument to posit that even beyond what at the time people referred to as "cyberspace", "code is law" (1998, p. 553). This argument was most forcefully extended by Lessig (1999), who famously argued that computer code regulates human activity in much the same ways that law does. Such concerns persist in much contemporary technology criticism. There has been a raft of scholarship pointing to the ways that technology companies like Google exert undue power over the ways people interact with their cities (cf. Ford & Graham, 2016; Graham et al., 2013). A similar fear underpins much critical scholarship on "smart cities" (cf. Greenfield, 2013) in which digital infrastructures impose hegemony on urban life, shaping what is possible and what is not in the smart city. To be sure, this unidirectional vision is balanced by long-standing arguments such as Graham's (1998) recombinatory and relational melding of cities, space and information (see also Hillis, 1998; Kitchin, 1998).

Second, Kitchin and Dodge (2005) focus on how code and materiality combine to create what they characterise as "code/space" and "coded space". Code/spaces are sites in which code dominates the production of space. Coded spaces, in contrast, are sites in which code is incidental to the production of space. In this theorisation, the central question is how materiality and code co-constitute places in an ontogenetic process as places are continually brought into being with code

as a key (although not always dominant) factor in place-making. Kitchin and Dodge emphasise that the role of code in shaping space is neither deterministic nor the same in all contexts; rather they argue that code/space

is contingent, relational, and context dependent. Code/space unfolds in multifarious and imperfect ways, embodied through the performance and often unpredictable interactions of the people within the space. (2011, p. 18)

In other words, code/space emerges in response to a relational problem – how to move someone from point A to point B, how to augment an urban experience – but the solutions offered by code/space are always partial and superseded by the next instantiation of code/space. Moreover, even though software acts as a catalyst for transducing space (bringing space into being), its effects are neither absolute nor universal. Rather the solutions turn on how people interact with one another, the physical space and the code. This formulation represents an important nuanced approach to the interaction of code and materiality and highlights the diversity of possible arrangements and outcomes.

Third, and relatedly, Graham et al. (2013) and Zook and Graham (2007a, 2007b) focus on the immaterial informational layers that augment everyday spaces and the power these augmentations have over representation. In this formulation, it is not just code, but also layers of digital information (e.g., Wikipedia articles, Yelp reviews, content in Google Maps etc.) that are as integral to a place as the bricks, mortar, steel and glass that make up its materiality. Particularly key is that with the advent of mobile computing, these digital layers are accessible and editable by people in situ making information and code key elements in dynamic place-making (Graham et al., 2015).

All three approaches stress that the digital and material are not operationally separate spaces but intricately entangled, both shaping and being shaped by one another. The latter two approaches also highlight the contingent nature of code/spaces and how they are ever more unfixed and hybridised. Said differently, spaces and the human interactions that create them are continually constructed and reconstructed with the aid of information technologies (Graham, 1998; Latour, 1987). This all sharply contrasts with more restrictive formulations where code proscribes with the power of law.

### 3 | RELATIONALITY AND RESISTANCE IN CODE/SPACE

This dynamic and unbounded formulation of code/space follows Massey's (2005) conceptualisation of relational places, always-ephemeral constellations or bundles of space-time trajectories. Kitchin and Dodge characterise code/space in a similar manner as “diversely, multiply, and ceaselessly scaled . . . self-organizing systems of relations stretched out across space and time” (2011, p. 77). For example, the digital networks of ATMs necessarily connect to certain material locations to dispense cash but are also connected to global information systems and the code/space involving a cash withdrawal is enacted across all these interconnected scales. Thus far, however, research on code/spaces has focused more on the experience of particular sites – the ways in which code is embedded in the home or the specifics of the digital augmentation of city streets – and less on the relational dimension of these hybrid spaces.

However, developing what Massey (1991) termed “a global sense of place” about these hybrid spaces is key for code/space research. Most importantly it affords the possibility to think more systematically about “power-geometries” that span our planet: the ways that the actions of people in one place are tied to other people thousands of miles away (for instance, the buying of a phone in Copenhagen will impact the life of a rare earth miner in Congo – and vice versa). Successfully attending to the relational aspects of code/spaces is difficult and the approach we use in this paper – calling out moments when relational connections are particularly visible and how individuals' actions shift power and even victimise others – is an imperfect but important technique in highlighting the relationality of code/spaces.

#### 3.1 | Resistance and transgression

In addition, we argue that some analyses of code in everyday life have over-emphasised its power. While understandable given the need to demonstrate the relevance of a new field of inquiry, it has also served to black box the effect of code as relatively impossible to influence by those who live under its influence. In contrast, we argue that far from being hegemonic (Greenfield, 2013) or a set of laws (Lessig, 1999), the code within code/space, as Kitchin and Dodge argue, can be subverted as it has “cracks that allow unintentional sociospatial relations and formations” (2011, p. 75). In short, despite code's power to constrain – denying credit via a FICO score, enforcing a no-fly list or stigmatising “low-value” places – the algorithms that make up code/space are not all-powerful; resistance and transgression are possible and evident. Thus,

researchers need to better understand the opportunities for individuals and groups (not everyone is afforded the same opportunities) to negotiate the transduction of code/space, particularly when it undermines the stated goals of the code without completely disrupting it.

For example, Kitchin and Dodge (2011, p. 155) focus primarily on the use of code by the state to conduct surveillance and control movement – border crossings, highway systems and air travel (Dodge & Kitchin, 2004). While noting that the movements of luggage and people are “more than ever before taken by systems that operate in an automated, autonomous, and automatic way” (Kitchin & Dodge, 2011, p. 137), they also argue that code/spaces within air travel are unevenly produced and contingent on the ongoing interactions of passengers, airline employees, security staff and code. In this way they strongly dispute Lessig’s vision of code as law and instead emphasise how human gatekeepers – primarily airline staff and security personnel – embody performative roles in which they constantly and subtly influence and interpret the transduction of code/space. Despite this focus on contingency and emphasising the “flaws in procedures and structures, and potential impacts and misuses” of these code/spaces, Kitchin and Dodge observe that there has “been remarkably little mass, organised resistance by individuals, unions, or activists” (2011, p. 155). We suggest that this observed lack of resistance is partially due to the fact that many subversive practices seek not to render code/space inoperable but to manipulate it for the benefit of the individual involved.

Long before the emergence of code/spaces, human geographers theorised and practised similar forms of subversion and resistance to capitalism that manipulate or complicate rather than directly disrupt systems and space. For example, Debord (1955) and the Situationists advocated Psychogeography to destabilise familiar understandings of the world, “drifting” through cities, uncovering layers of emotion obscured by routinised behaviour. By violating the expectations of efficient transit or way-finding, the Situationists destabilised norms of permitted behaviour allowing for more playful engagement with the urban environment. Lefebvre’s (1968) “right to the city” also emphasised the disruptive power of alternative action that demanded “a renewed access and self-management of resources, surplus production, and the urban core” (Shaw & Graham, 2017, p. 1). Lefebvre’s right to the city is not a vision of rights bestowed, but one in which residents take active roles in the self-management of their lives. Said differently, exercising a “right to the city” that transgresses against hegemonic visions – originating from capitalist managers or code/space – requires residents (or users) to take matters into their own hands.

This kind of transgressive interaction with space is echoed in more recent actions by “urban explorers”, individuals who gain unauthorised access to the built environment in order to find “deeper meaning in the spaces we pass through every day” (Garrett, 2013, p. 6) such as “briefly brushing against the infinite while right in the middle of the city” (Garrett et al., 2016, p. 5). Finding meaning via destabilising engagements with everyday systems and spaces is also evident in ludic geographies that emphasise the “transformative potential” of playfulness, including “playing with limits, experimentation with rules, roles and meanings, and mimetic behavior” (Woodyer, 2012, p. 322). Related approaches such as games and gamification – the use of play or rewards to motivate behaviour – can also seek to rewire practices to resist capitalism and its spaces (Fuchs et al., 2015). These transgressions confound the centres of control in capitalist networks, shifting benefits (and harm) but in ways that often fall short of political resistance and liberation movements.

### 3.2 | Hacking as transgressions to code/space

Building on this heritage, we argue that hacking code/spaces – manipulating for subversion rather than inoperability – represents a key moment of transgressive power within modern society. Coleman refers to hacking as “a site where craft and craftiness converge” (2016, p. 161), also understood as a clever and non-obvious solution to problem-solving especially related to gaining access to resources (often digital). The term comes from computing and Levy’s (1984) characterisation of hackers as prioritising open information, deconstructing systems and community sharing. Central to this definition and actual practice is that the motivation for hacking is not necessarily a political project that easily conforms to offline activism or resistance. Despite this apolitical bent, Coleman argues that hackers’ actions are transgressive in that they represent cooperative projects that “experiment in the making of a social commonwealth; it is there where the hard work of freedom is practiced” (2013, p. 210). This produces a “particular geography of resistance” (Coleman, 2014, p. 393), such as the decentralised network used by the hacker group Anonymous that coalesces around various projects driven by emotive energy (e.g., exposure of a gang rape) via available cracks in computing systems (lax password security and low-cost distribution). According to Coleman this structures resistance so that



short-term power is achievable for brief durations, while long-term dominance by any single group or person is virtually impossible. . . . In this way, the multitudinal ‘nature’ of Anonymous precludes its subjection to either aspirational figures working internally, or external figure. (2014, pp. 393–394)

In other words, hacking can temporarily subvert or redirect attention, resources or rules by exploiting cracks in computer systems to achieve short-term goals. The selection of these goals, however, need not be driven by desire for democratic process, inclusivity or avoiding harm, making outcomes quite uneven and even potentially injurious to individuals only peripherally connected to the ostensible aim of an action.

Importantly for this paper, these analyses of hacking emphasise the ethos and organisation of this practice rather than the technology, suggesting that hacking extends beyond the manipulation of computers. For example, Garrett (2013) calls the practice of urban explorers “place hacking” (see also Dodge & Kitchin, 2006). This kind of hacking also prioritises information-sharing and community and focuses on understanding how systems – in this case the built environment of cities – fit together and how one gains access to parts that are normally closed off (Garrett, 2013). While the motivations behind hacking can be diverse – exploration, personal satisfaction, reputational enhancement, etc. – its continued and expanded use echoes long-standing social practices (DeBord, 1995; Lefebvre, 1968). Moreover, while urban explorers primarily see their motives as apolitical, the transgressive nature of them imbues them with politics because they allow one to “rethink not just one’s own identity but also the relationship between power and urban space” (Garrett, 2013, p. 8). Thus, to hack is to transgress and thereby actuate a moment of power relative to the larger capitalist structures in which we live. Even when hacking – be it creating free software, accessing and distributing incriminating materials, drifting through a city or playful mischief – is not deemed overtly political by its practitioners, the transgressive power and ethical concerns remain.

Given its transgressive power, the practices and ethics of code/space hacking of the economy and everyday life becomes of fundamental interest. Like other hackers, code/space hackers seek to understand how systems function (in this case how the material world and code are combined via algorithms) in order to access restricted spaces of direct interest or benefit for them. Whereas computer hackers might use scripts to search for unsecured computer ports and space hackers might hop a fence to enter an abandoned factory, code/space hackers alternatively use digital and material elements to access the opportunities and offerings of the hybrid spaces of our economy and everyday lives.

#### 4 | CODE/SPACES OF AIRLINES AND FREQUENT FLYER PROGRAMMES

The contemporary system of global airlines operates as a complex assemblage of code, machines, nature and people. It is “perennially open to new spatial configurations and unanticipated lines of flight” (Lin, 2014, p. 233) resulting from human intervention, natural events and the function or failure of digital and material equipment. These systems are in constant flux – what Lin (2014) refers to as remobilisations of anticipatory assemblages – as various inputs create new aeromobilities. While some of these inputs are clearly beyond human control (wind patterns or volcanic ash clouds), others are deeply imbricated with code. Everything from pricing, to purchasing tickets, to tracking luggage and boarding procedures relies on information technologies to produce code/spaces in which routine decisions are handled by algorithms, with little intervention by humans. In short, the code/spaces of global air travel are encoded by digitally mediated systems of governance. These spaces are primarily designed to maximise company profits via dynamic pricing, routing rules and ancillary fees, but also seek to build customer loyalty through the targeted distribution of benefits such as upgrades for elite customers or complimentary flights via frequent flyer programmes (Derudder et al., 2010; Gössling & Nilsson, 2010).

Frequent flyer programmes date back to the 1970s as airlines sought to track and reward their customers in the post regulation era. Since that time, trillions of miles have been awarded (The Economist, 2005) and hundreds of million people have joined these programmes. Frequent flyer programmes change overnight with scant recourse for members: after all, programmes come with defined terms and conditions written in the interest of the airline. Among other things, these terms specify that miles are not the property of the member (a point held up by case law), are subject to confiscation for misuse (such as selling a reward seat) and the terms for earning and redeeming are subject to change at any time; in short members beware! While these programmes were originally limited to earning and redeeming via flights, they have grown in complexity as marketing departments devised new ways for consumers to earn and redeem points via hotel stays, purchases and credit card applications. Airlines also use code to automate the release of reward space to their frequent flyer programmes, a process governed by impenetrable rules and restrictions (at least from the perspective of most consumers) in which algorithms possess all the power and seemingly leave little opportunity or agency for users.

Although airlines designed frequent flyer programmes in their own interests, these code/spaces are vulnerable. Ironically, the same algorithms required by airlines to function simultaneously provide the means for a relatively small number of airline hackers<sup>2</sup> to reconfigure the code/space of frequent flyer programmes to their own advantage. In their analysis of the role of code in air travel, Kitchin and Dodge (2011, p. 74) argue that in the transition zones of airports – boarding, security, passport control – “the visible transduction of code/space is magnified” while in other areas – the departure lounge, in the air or in baggage claim – the role of code is backgrounded. While we agree that transition zones are intense moments of code/space, we also emphasise the role of code (as well as the ability to hack this code) in shaping these other moments as well. For example, the ability to access private lounges, whether one is seated in a premium cabin and even the order in which one’s bags emerge on the turnstile are all transductions of frequent flyer code/space. While much less visible than passport control, these sortings take place constantly.

## 4.1 | Ethics and research methods

Our interest in airline hacking began as hobbyists motivated by a desire to enhance our aeromobility (Gössling & Nilsson, 2010), which we achieved via award redemptions for over 100 tickets on more than 20 airlines<sup>3</sup> and approximately 75 nights at major hotel alliances. Thus, rather than the idealised disinterested (and largely fictitious) researcher approaching a topic *de novo*, we are messily bound up with our work, which brings several advantages. First, it is only through our hobby that we became aware of the novel theoretical implications of a kind of hacking that transgresses and manipulates but does not completely disrupt code/space. Second, our activities as hobbyists – ten years of participant observation including posting in newsgroups and blogs as well as experimenting with point collecting and redemption techniques – gives us a depth of understanding equivalent (if not surpassing) most time-limited academic fieldwork. Finally, our long-time presence in hacker networks gave us access to key non-public networks used by the most sophisticated actors to share closely guarded deals.

While absolutely fundamental to our ability to conduct this research, we readily acknowledge that our participation in and benefit from airline hacking also brings ethical concerns about legality, morally debatable actions, impact on others and even contribution to global climate change. The first issue is also the most easily addressed: we never engaged in any illegal activity during this research. These programmes are regulated primarily as contracts, generally written to give airlines considerable power over consumers (Leff, 2014a), and thus questionable activity would be a breach of contract rather than illegal. That said, we never engaged in (or were accused of) any breach of contract.

In terms of the second concern, our comfort with the mortality of our actions is based in the decidedly ambiguous and often contradictory attitudes towards frequent flyer promotions that emerge from complex organisational structures often at cross-purposes. Marketing and public relations departments use frequent flyer programmes and points to build demand and brand awareness, while scheduling and yield management departments seek to maximise revenue. This can lead to accusations of false advertising from consumers who are unable to use points as they had expected, and conversely to airline managers accusing hackers of misusing the system.<sup>4</sup> In other words, expectations for how one should participate in frequent flyer programmes are varied, contested and evolving, with airline managers engaging directly and positively with hackers (online and at specialised conferences) while simultaneously revising programme rules to restrict benefits without levelling accusations of immoral use.

That said, travel hacking has relational impacts that go beyond the immediate, contributing to larger, and at times detrimental, outcomes for others. We have no ready response to this and recognise the paradox of our hacking in which our transgressions against these corporate systems have implications for people who will never fly. These relational implications, however, are also true for all economic decisions in global capitalism. Therefore we seek to meet our ethical obligation as researchers by clearly highlighting moments at which our actions have impact, however diffusely. Finally, it is important to acknowledge the contribution of air travel – particularly business and first class seats given their larger footprint – to climate change. While all air travel is entangled in this ethical issue, the travel resulting from our hacking resulted in little marginal increase to carbon output as award seats are those that airlines do not expect to sell, the flight itself will take place with or without the redemption. Moreover, precisely because they are non-revenue these awards do not contribute to airlines’ demand models that shape scheduling and aircraft decisions.

Key resources for this research were airline hacker message boards that distribute and archive this community’s discussions. The primary message board we consulted was FlyerTalk.com, started in 1998, although we also tracked InsideFlyer.com (formerly known as MilePoint), FatWallet.com and the sub-reddits on Frequent Flyer miles (<https://www.reddit.com/r/frequentflyermiles/>) and credit card churning (<https://www.reddit.com/r/churning/>). While message boards remain a key site of activity, bloggers began to establish their own sites in the early 2000s. From the dozens of available blogs, we focused our attention on a few, including ViewfromtheWing, OneMileAtATime and ThePointsGuy as these represent some of the largest and most



influential actors, regularly discussed on message boards and quoted by mainstream media. These were supplemented by more limited readings of other more specialty-focused blogs, including MommyPoints, TheFrequentMiler and the FrugalTravelGuy. While some hacking techniques are global (creative award redemption and mileage running), the US regulatory and marketing environment make earning points for non-flying activities particularly lucrative. As a result, our empirical cases, selected based on our knowledge of popular tactics, are relatively US-centric (although similar opportunities do exist in many European and other countries). We have comprehensive records of our own activities for earning and redeeming miles and kept careful notes on our experiments with a wider range of hacker tactics to verify their validity and evaluate the relationality and spatiality of each practice.

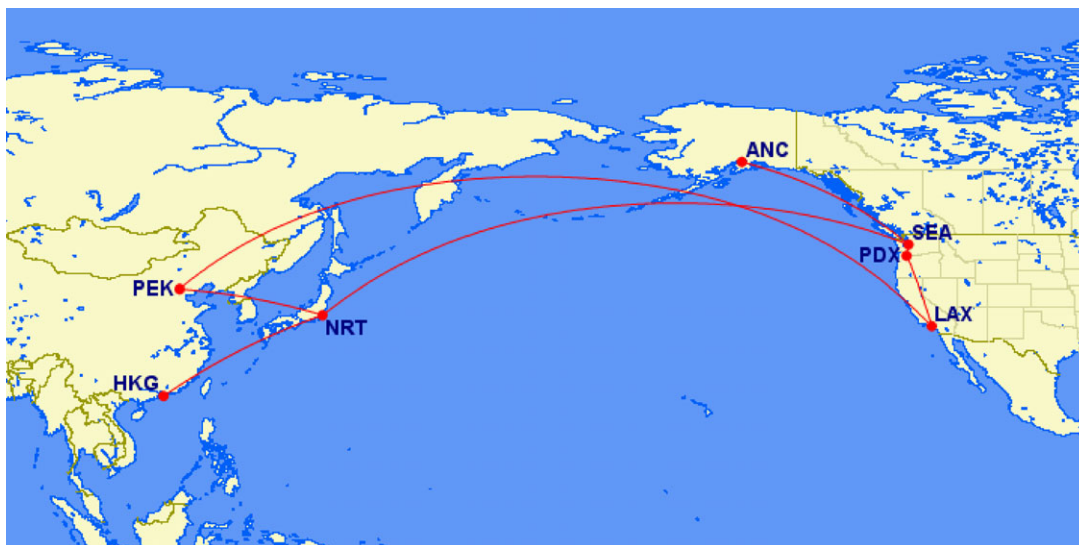
## 5 | TRANSGRESSIVE PRACTICES OF AIRLINE HACKERS

The ways most frequent flyer members earn miles – flying, airline credit cards and marketing bonuses – are similar to strategies used by airline hackers, albeit differing by an order of magnitude in scope and scale. This review highlights three key hacking techniques – creative use of airline geographies, credit card churning and consuming for miles – focusing on the relationality and spatiality of these code/spaces. While these tactics are theoretically available to anyone, they work best for individuals with lifestyle privilege, e.g., higher incomes and flexible schedules, and our interactions with the airline hacking community suggests a strong skew in gender (towards men) and race (primarily white) within the demographics of participants.

### 5.1 | Creative use of airline geographies

One of the simplest techniques for airline hacking is understanding how the algorithmic rules – particularly regional definitions – defy material geography and shape particularly advantageous awards. For example, the BMI<sup>5</sup> airline defined all of Russia as Europe and one could book a one-way “inter-Europe” award from London to Vladivostok (in East Asia). By routing via one’s actual destination, e.g., Seoul or Tokyo, and not taking the last leg to Vladivostok, one could travel for many fewer miles than an actual Europe to East Asia award required. A similar example was the so-called “sweet spot” in US Airways awards that priced a USA to North Asia business seat award (which allowed for a stopover in Europe) at 10,000 miles less than a straight USA to Europe award (Schlappig, 2013).

The most creative use of airline geographies is mileage running, booking low-cost, long-distance flights (often based on pricing errors coded in booking software) and/or routing trips in a circuitous manner. The goal is maximising mile earnings relative to cost, making the destination largely incidental; many of these flyers never leave the airport. This technique



**FIGURE 1** An example of a mileage run routing.

*Source:* Informant’s example of a mileage run from 2011 for a round trip from Portland (PDX) to Tokyo (NRT) that included stops in Seattle (SEA), Anchorage (ANC), Hong Kong (HKG), Beijing (PEK) and Los Angeles (LAX) to maximise miles; Map from Great Circle Mapper, <http://gc.kls2.com/> [Colour figure can be viewed at [wileyonlinelibrary.com](http://wileyonlinelibrary.com)]

exploits airline routing rules that allow multiple legs via connections that are immediately illogical to a human observer (see Figure 1) but perfectly rational in the code/space of airline bookings. This is fairly common behaviour within the airline hacker community with over 55,000 threads and 967,000 posts at the Flyertalk forums dedicated to it.

Pricing is key, as many mileage runners will not book a flight unless it earns a specific cost per mile (CPM).<sup>6</sup> This leads some to buy tickets originating from peripheral locations (e.g., Cairo, Egypt or Colombo, Sri Lanka), as they are considerably less expensive than those beginning in the global centre (Schlappig, 2014). Cost concerns also means that mistake fares filed by airlines are highly prized. Examples include misplaced decimal points making fares a tenth or hundredth of the intended amount, or incorrect currency listing such as an Alitalia US\$3,300 business class fare from Toronto to Cyprus that briefly sold for US\$33. As in the case of flight routing, a human travel agent might identify such a fare as worthy of further investigation, but online booking engines simply proceed with a booking. In response, airlines have developed new, error-checking software and rely on regulatory agencies (such as the US Department of Transportation) to ensure that in “mistaken fare situations” they could raise prices or cancel tickets (Leff, 2015).

A related hacker strategy is known as “fuel dumping”, or avoiding hundreds of dollars in fuel surcharges. These extra fees are automatically priced based on regional classifications and airline interline alliance agreements and adding the right final leg to an itinerary can trigger an error and prevent the surcharge. Since the algorithms did not consider the actual spatiality of travel, short, inexpensive flights, e.g., adding a flight from Miami to the Bahamas to the end of a round trip between Newark and Madrid, were favourites (The Economist, 2013), creating relational connections between distant operations. Airline hackers worried that too much attention would compel airlines to fix these errors; as one blogger notes, “Airlines know about ‘fuel dumps’ and for the most part they are obscure enough and low volume enough that they aren’t a priority to deal with” but “broad use of specific technique will raise the cost to the airline of that technique, and raise the priority to close the ‘loophole’” (Leff, 2013, np).

To illustrate how this works in practice, we offer an example we received from an informant connected to a private hacker network dedicated to sharing pricing errors and fuel dumps.

Email from Airline Hacker<sup>7</sup>

Wake up . . . and keep it under wraps. From the secret net, so far it hasn’t hit FT. It’s going to die immediately when that happens so check it out if interested. This one from TPE. TG filing TPE-LAX. As low as \$400 a.i. for a straight TPE-NRT-LAX routing or \$650 or less for TPE-HKG-BKK-NRT-LAX. All routes show TG codeshare on the TPAC (NH 773). You need to use x.nz . . . to book. . . . You can’t find it on x.com or x.co.uk. . . . Mine goes TPE-HKG-BKK-NRT-LAX and gives me the F suites on the TGA380 and the F suite on the NH 773 for the TPAC sector. And the F suites on the EK 380 with the in-flight shower. EK doesn’t credit to useful programs for me, but the rest will. I only have J on the CX sector to HKG but, oh well. . . . Mine ticketed via x.nz on TG stock within 30 minutes. I’ll worry about fuel-dumping the westbound TPAC for TPE later. . . . I need 100k UA miles yearly to feed the status monster. If you don’t have UA status, then the run will be a net negative. In my case, with the COS multipliers (250% RDMs for paid F on NH when crediting to UA, for example) plus the 100% 1K bonus on the Star legs, I will recover about the 32.5k MP miles that a one-way positioning award would cost if I use an award. I’ve got ten months to wait for a cheapie TPAC in the meantime. . .

This message outlines a fare mistakenly filed by Thai Airlines (TG) for first class travel from Taipei (TPE) to Los Angeles (LAX) via Tokyo (NRT) for US\$400 or via Hong Kong, Bangkok and Tokyo (HKG-BKK-NRT) for US\$650 (earning more miles). The hacker took special care in selecting specific aircraft (with desirable amenities) including a Boeing 777-300 from All Nippon Airways (NH 773) and Airbus 380s from Emirates Airlines (EK380) and Thai Airlines (TGA380). It is only possible to book this flight at Expedia.co.nz (x.nz); the code used by the US (x.com) and British (x.co.uk) versions of the same platform do not have this error. The hacker outlines his main motivation, retaining airline status made easier because of the extra miles (250% RDMs) he will earn due to his travel class (COS multipliers) and current status (100% 1K bonus). He also looks forward to experiencing on-board luxury – including a joking lament that he only has business class (J) on Cathay Pacific (CX) for one leg – and achieving a highly mobile lifestyle (see Gössling & Nilsson, 2010). He also notes his strategy to position himself in Taipei for this flight, either a one-way positioning award or a cheap transpacific flight (TPAC) made possible by fuel dumping.

This message shows the techniques for mileage runs – only possible with certain origin cities or via certain booking platforms – as well as their complexity (possible routings, airlines and aircraft across the entire Asian region) are brought

together in an ephemeral moment of code/space, shaped by a fare calculation algorithm. Most importantly, it highlights the complex priorities governing hacker networks and the code/space in which they operate. Our informant's first point is emphasising the need to keep the fare secret; there are cracks in code/space but if they are pushed too wide and used by too many people, they will cease to exist.

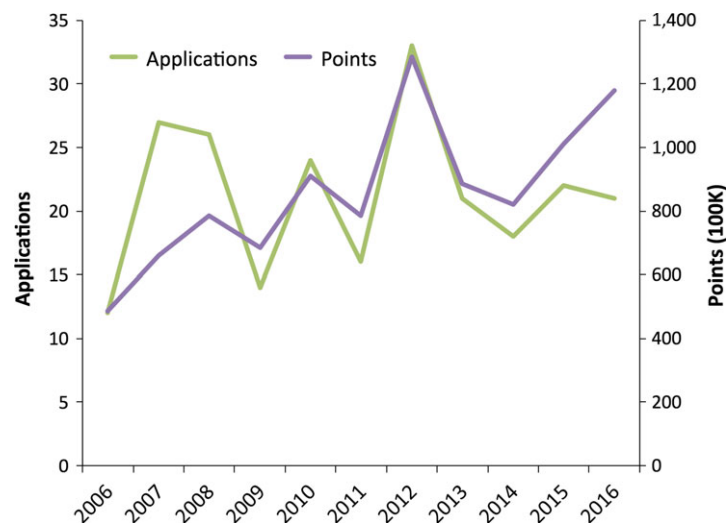
## 5.2 | Credit card churning

Banks (and other airline partners, including rental car and hotels chains) purchase the majority of airline miles issued each year – 65% in the case of American Airlines (American Airlines, 2015; Leff, 2014b) – providing important revenue streams to these companies (Edmonston, 2009). This makes repeated applications for airline branded cards (or churning) a standard practice for airline hackers. The algorithms used to evaluate applications were designed with the assumption that getting a credit card would be a rare event for each consumer and therefore it was only recently that banks began limiting the number of applications from any individual. For example, one of the authors (and spouse) amassed 10 million miles/points (spread across a number of airlines, hotel chains and other reward programmes) by applying every month for 11 years for a total of over 235 credit cards (see Figure 2). This level of churning is matched (and exceeded) by other hackers; in 2013 the FrequentMiler blogger amassed one million miles in a month with over half the points coming from credit card bonuses (FrequentMiler, 2013).

Credit scores, such as the FICO, designed to assess the risk of debt repayment algorithmically, play a central role in churning. Those with high FICO (or equivalent) scores automatically receive approval for new credit at competitive rates, while those with mid-range or low scores face more onerous terms or outright denial. The geography of credit card churning is extremely differentiated because United States residents are tempted with bonuses of 50,000 or even 100,000 miles while offers in other countries are either non-existent or in the order of 10,000 miles or less. Thus, airline hackers rely on a particular constellation of code/space based in the *laissez-faire* regulatory environment of the USA that includes high credit card use among consumers which generates merchant transaction costs (approximately 1.5%) with each purchase and often accruing late fees and interest payments. The resulting profit centre relies on all credit card-using consumers regardless of whether they fly and is essential for fuelling generous marketing bonuses that makes churning so lucrative, at least in the USA.

## 5.3 | Consuming for miles

Another hacking technique is leveraging marketing campaigns that offer free miles for purchases. A famous example is David Phillips, who acquired 1.2 million American Airline miles at a cost per mile (CPM) of US\$0.0025 by buying Healthy Choice pudding cups (Phillips, nd). Other marketing campaigns – Emmi Swiss Knight Gruyere Cheese containing a coupon for 500 American Airline miles – have also caught the attention of hackers. Although less of a bargain than



**FIGURE 2** Yearly counts of credit card applications and award points earned by author; 2016 data is as of August. [Colour figure can be viewed at [wileyonlinelibrary.com](http://wileyonlinelibrary.com)]

pudding cups, the CPM of US\$0.012 was still attractive enough for five Flyertalk users – including one of the authors – to form a buying consortium to purchase 1,260 wheels of cheese (Flyertalk, 2006).

Although the goal of this transaction was frequent flyer miles, the spatiality and relationality of its code/space was quite complex, including negotiation among the consortium members who had never met and the material logistics of shipping, receiving, storing, extracting the coupons (see Figure 3), submitting the paperwork to the vendor and disposing of the cheese. Once processing was completed, there remained the very material issue of storage and disposal of the by-product (50 kg of cheese that might be referred to as an “acquired taste”). Indeed, this was a considerable problem – many acquaintances were “gifted” with unexpected bags of cheese – demonstrating the intricate intertwining of material and digital spatialities in code/space.

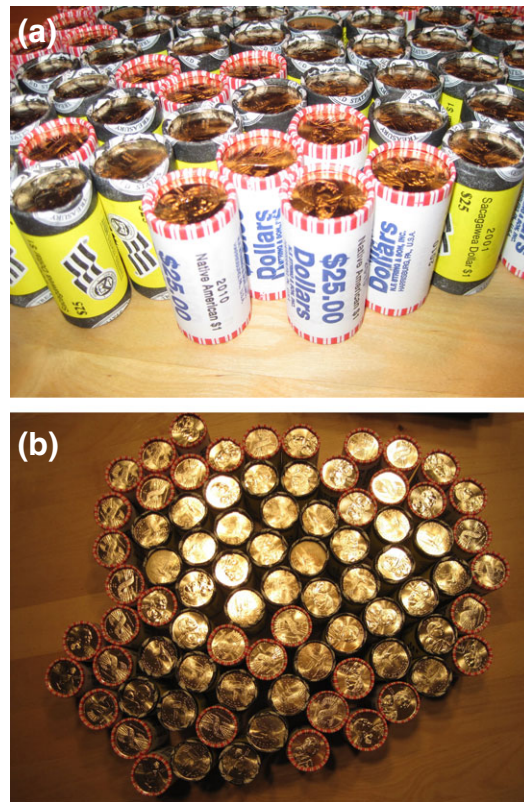
Hackers also engage in manufactured spending, using a mileage-earning credit card to purchase cash equivalents or easily liquidated items. Purchasing dollar coins from the US Mint was long favoured by hackers, because shipping was free in an attempt to get these unpopular coins into circulation (Dolen, 2011) and they were coded as a purchase rather than a cash advance (Flyertalk, 2009). This allowed hackers to earn miles for spending but have ready (albeit unwieldy) cash to pay their credit card bill. Some participants reported ordering tens of thousands of coins a day (Mr Pickles, 2011) before the US Mint stopped accepting credit cards for payment (Dolen, 2011; Flyertalk, 2009). A limited field test by the authors confirmed the viability of this strategy (see Figure 4), although also demonstrated the material burdens of its spatiality. While purchasing 2,000 dollar coins only required a few clicks, prudence mandated being physically present for delivery and depositing 16 kg of coins involved considerable time at a bank. Some banks reportedly limited deposits of coins given their unpopularity and burdensome nature and hackers would distribute deposits across branches to avoid receiving too much attention (Flyertalk, 2009).

Airline hackers also use other products that do not code as a cash advance – money orders, gift cards and prepaid credit cards – to earn miles. The authors tested this strategy, but the effort and risks associated with repeatedly physically moving large amounts of cash or cash equivalent was prohibitive. This strategy has grown increasingly difficult as many of the preferred products (Vanilla Reloads, REDbird), vendors (Staples, CVS) and banking networks (Bluebird, Serve) have enacted



**FIGURE 3** A selection from 50 kg of cheese purchased by author to obtain American Airline coupons. [Colour figure can be viewed at [wileyonlinelibrary.com](http://wileyonlinelibrary.com)]





**FIGURE 4** US\$2,000 in dollar coins purchased from the US mint by author. [Colour figure can be viewed at [wileyonlinelibrary.com](http://wileyonlinelibrary.com)]

policies to increase costs in an effort to stop this activity (FrequentMiler, 2016). These changes also mark a key moment in the relationality of frequent flyer code/space as many of these products (e.g., American Express' Bluebird network) were designed for low-income customers who now also face increased costs and hassle although they may never fly. Another example of the unanticipated relationality and spatiality created by hacking is evident at the micro-lending non-profit Kiva.org. Using mileage-earning credit cards, frequent flyers have loaned over US\$12 million in capital to entrepreneurs in developing countries, making them the third largest group active on the site, with lending rates that are ten times the average amount (Kiva, 2016).

These unexpected interconnections and impacts created by hacking – be it increased costs to the unbanked or capital flows to an entrepreneurial class within the developing world – are hard to generalise. These transgressive practices do not simply produce resistance to algorithmic control or impact the profit margins of airlines or banks. Instead, the impacts can be diffuse and uneven with benefits accruing primarily to hackers and negative effects going to others who are relationally connected, although extremely peripherally. The relationality of code/space is also evident in the real costs of these activities to vendors – Staples, CVS, US Mint – who have no connection to the airline industry at all. This point is emphasised within a public Reddit (2016) thread: “while you reap the rewards from manufactured spending, someone else loses money in the process (usually whoever pays for the credit card transaction fees)”. As a result, many of the manufactured spending strategies are closely guarded secrets and again illustrate the conflicting priorities of frequent flyer hackers: sharing how code/space can be manipulated but recognising that, if pushed too far, the relational distribution of costs may elicit a response that closes the cracks.

This is a valid concern because as airline hackers rewrote the code/space of frequent flyer programmes, the managers and designers of these systems reacted. Airlines took harder lines on mis-filed fares popular with mileage runners and frequent flyer programmes devalued points, tightened routing options and increased fees – changes that affected regular flyers and programme members in addition to hackers. Banks began limiting the number of credit card applications, and marketers (of pudding, cheese and other products) took greater care in structuring promotions. While hackers lamented specific changes, they did not stop; rather they reworked their tactics to manipulate the current moment of code/space. While the particular examples discussed here may no longer be possible, they aptly demonstrate the relational and spatial contours of code/space hacking. Even when managed by multi-billion dollar corporations, the code and algorithms of code/space are not truly hegemonic. Instead code/spaces are ontogenetic places, continually brought into being by the interaction of

materiality and code, sometimes as envisioned by its designers but also via unexpected transgressions that reverberate unevenly across the networks of capitalism.

## 6 | CONCLUSIONS

The global airline network is a key code/space of contemporary global capitalism and, like other core networks, relies on a heavy degree of algorithmic (albeit non-hegemonic) governance. Crucially, this analysis shows that the encoded rules and algorithms of airlines are potentially malleable via the practices of hackers that “offer an abstract negation that doesn’t already fit into a binary computation” (Shaw & Graham, 2017, p. 917); they refuse to act in the ways that algorithms and systems define as normal. These efforts demonstrate that the very complexity of code/spaces can render systems designed for hegemonic control porous and susceptible to subversion by those it was meant to restrict. The diverse and colourful examples from airline hacking highlight both the myriad ways a system has been turned towards unintended purposes and the creative (and time-consuming) methods some will use to manipulate code/space for their own goals. In short, these transgressions demonstrate that we need not do everything that the machines tell us to do.

To be clear, the case of airline hackers is not necessarily a subversive or even democratic activity as the motivations and effects are focused on personal gain. Encoded rules often exist for good reason and thus hacking is not inherently emancipatory (Mott & Roberts, 2014), and has the potential to undermine well-intentioned and socially beneficial systems. However, our analysis demonstrates how playful, transgressive and mischievous approaches can repurpose and recreate the code/spaces of airlines and beyond.

In addition to computer hacking documented by Coleman (2013, 2014), individuals regularly remake elements of their hybrid spaces.<sup>8</sup> Examples include Google bombing or search engine optimisation (SEO) that manipulate search results, as well as virtual private networks to gain access to online material blocked because of one’s location. Other practices target tracking and profiling systems by flooding them with false data using readily available tools like the AdNauseam.io browser plug-in that clicks on all advertisements to mask users’ habits. While these cases began as exclusively digital practices, the hybridisation of space – e.g., search engine optimisation of maps (Zook & Graham, 2007a, 2007b) and profiling users by tracking physical mobility (Conger, 2016) – ensures their relevance to material and code/spaces.

There are also micro-hacks in public transportation systems in most cities worldwide: solutions that save time or money using strategies not envisioned by transport planners. Londoners, for instance, pay fares based not on distance travelled, but on how they traverse concentric fare zones radiating outwards from the centre. However, there is one particular Overground rail line that travels from the west to the east of the city without leaving one of the concentric zones: allowing canny travellers to traverse huge distances for the cost of a local journey. Opportunities for code/space hacking are growing as the Internet of Things (IoT) and smart cities initiatives increasingly surround us with devices that exert control over our spaces but often do so rather insecurely.<sup>9</sup>

As code increasingly governs financial transactions, human mobility, dating, job search and much of the rest of everyday life, a key finding of this paper is recognising the potential vulnerability of even the most encompassing algorithms. Code often works on people, en masse, expecting them to act in normal and foreseeable ways. But in a world of unpredictable people, able to engage with, transgress against and switch between networks, the hegemony of code/space can be contested and manipulated. Algorithmic rules for human behaviour often do produce socially valuable outcomes, and they might find us the perfect job, partner and mortgage; but they also restrict choices, force disadvantage and disempower the individuals that they govern. It is hard to argue with an algorithm, or even ask it why it made the choices that it did. Airline hackers, through craft and self-interest, exemplify the ways we might manipulate code to challenge the power of code/space to shape human behaviour. In an age of smart cities, big data and encompassing surveillance systems, there seems little doubt that hacking efforts will expand to other areas of digitally mediated daily life.

The trickery of hackers, however, is not devoid of its own power and ability to negatively impact (often unknowingly) those to which it is relationally connected. Hackers can certainly transgress against corporate systems, but the reaction to these challenges reverberate through the global networks of capitalism. This ultimately points to the need for an ethics of care that recognises the relational economic positionalities that we share with one another. The code of everyday life is malleable, but efforts to sidestep and subvert it enrol us into uncomfortable power-geometries beyond our immediate space-time horizons. Thus, we all have a responsibility to reflect on not just the power of code, but also the power we exert through it, with it and because of it.



## ACKNOWLEDGEMENTS

The creation of this paper would not have been possible without the help from a variety of friends, colleagues, and large corporations who occupy various niches in the global airline ecosystem. We would first of all like to thank a range of anonymous informants – especially Keiron Bailey – for their insights, hacks, trips, tricks, and general willingness to forge their own code/spaces. We also wish to thank the [three?] anonymous reviewers who greatly helped to sharpen the ideas in the paper into their current form. Support from a Philip Leverhulme award helped to support the writing of the paper. Frequent flyer programs, airlines, large banks and cheese merchants all (unknowingly) made some of the “fieldwork” possible in their own ways. Finally, we wish to thank our partners and family, who have long supported our airline hacking habits including assistance in field-testing various collection and redemption tactics.

## ENDNOTES

- <sup>1</sup> This paper uses the term “code” to refer to software and computer languages. It also uses the term “algorithm” to refer to a set of operations or rules (often mediated by code).
- <sup>2</sup> There are no figures on the number of practising airline hackers. The oldest and largest message board used by the community – flyertalk.com – has over 650,000 member accounts and the bloggers used in this research have follower bases on Twitter and Facebook that number in the tens of thousands. Including all these (even though many of these accounts/followers are unused) still makes this community less than 0.5% of all frequent flyer members.
- <sup>3</sup> These include Air France, American Airlines, ANA, Austrian Airlines, BMI, British Airways, Brussels Airlines, Cathay Pacific, Egyptair, FinnAir, Iberia, Japan Airlines, Jetblue, KLM, Malev, Lufthansa, Delta, Qantas, Singapore Airlines, South African Airlines, Swiss Airlines, Thai Airlines, Turkish Airlines, United Airlines and Virgin Australia to destinations worldwide.
- <sup>4</sup> For example, a US Airways senior marketing executive famously (at least within hacker circles) derided bargain hunters as “not necessarily the kind of loyalty we want to reward” (De Lollis, 2002). A number of USAirways members (and FlyerTalk regulars) found this objectionable and took to calling themselves “cockroaches” to lobby the airline for better treatment (or at least respect), ultimately achieving a face-to-face meeting with executives and a type of *détente* (Alexander, 2004).
- <sup>5</sup> Most of the BMI network was bought by International Airlines Group (British Airways) in 2012, putting an end to this unique interpretation of the boundaries of Europe.
- <sup>6</sup> The desired CPM rate varies between hackers, the type of miles gained (e.g., Delta SkyMiles or Singapore Krisflyer miles) and evolves over time, but most mileage runners require a CPM of US\$0.02 or lower.
- <sup>7</sup> See <http://www.flyertalk.com/forum/glossary.php> for definitions of the shorthand used here.
- <sup>8</sup> In addition to remaking code/spaces for personal gain or mischief, there are also significant efforts by activist hackers to not just work within the constraints of algorithms, but also to change, break or undermine them. Scholars such as Coleman (2013) and Jordan (2008) challenge ideas that hackers are simply lone-wolf individuals driven by a so-called “Californian ideology”. Their “craft and craftiness” is instead often grounded in collaboration and community and shaped by ethical principles and political commitments from across the ideological spectrum.
- <sup>9</sup> For example, road signs and sensors, smart buildings, close-circuit TVs, parking payments and industrial control systems all offer new vectors for hacking the code/spaces in which billions of people live (Beccaro & Collura, 2016; Conti, Cross, & Raymond, 2016).

## ORCID

Matthew Zook  <http://orcid.org/0000-0002-6034-3262>

Mark Graham  <http://orcid.org/0000-0001-8370-9848>

## REFERENCES

- Alexander, K. (2004). ‘Cockroaches’ US Airways worked to keep. *Washington Post*, 24 August E1 (<http://www.washingtonpost.com/wp-dyn/articles/A27394-2004Aug23.html>) Accessed 30 January 2017.
- American Airlines. (2015). American Airlines annual report. (Form 10K) ([http://phx.corporate-ir.net/phoenix.zhtml?c=117098&p=irol-sec&seccat01.1\\_rs=11&seccat01.1\\_rc=10](http://phx.corporate-ir.net/phoenix.zhtml?c=117098&p=irol-sec&seccat01.1_rs=11&seccat01.1_rc=10)) Accessed 13 February 2016.
- Beccaro, M., & Collura, M. (2016). (Ab)using smart cities: The dark age of modern mobility Presentation given at HITB GSEC. Singapore 22–26 August (<http://gsec.hitb.org/sg2016/sessions/abusing-smart-cities-the-dark-age-of-modern-mobility/#>) Accessed 30 January 2017.
- Castells, M. (1996). *The rise of the network society: The information age: Economy, society, and culture* (vol. 1). Chichester, UK: Wiley.
- Charette, R. N. (2005). Why software fails. *IEEE Spectrum*, 42, 36.
- Coleman, G. (2013). *Coding freedom: The ethics and aesthetics of hacking*. Princeton, NJ: Princeton University Press.
- Coleman, G. (2014). *Hacker, hoaxer, whistleblower, spy: The many faces of Anonymous*. New York, NY: Verso Books.

- Coleman, G. (2016). Hackers and the craftiness of craft. In B. Peters (Ed.), *Digital keywords: A vocabulary of information culture and society*. Princeton, NJ: Princeton University Press.
- Conger, K. (2016). Uber begins background collection of rider location data. *TechCrunch.com*, 28 November (<https://techcrunch.com/2016/11/28/uber-background-location-data-collection/>) Accessed 30 January 2017.
- Conti, G., Cross, T., & Raymond, D. (2016). Pen-testing a city White Paper from the Securing Smart Cities Initiative. (<http://securingsmartcities.org/wp-content/uploads/2016/03/Pen-Testing-A-City-wp.pdf>) Accessed 20 February 2017.
- De Lollis, B. (2002). US Airways' fare changes anger many. *USA Today*, 28 August.
- Debord, G. (1955). Introduction to a critique of urban geography. In H. Bauder & S. Engel-Di Mauro (Eds.), *Critical geographies: A collection of readings* (pp. 23–27). Kelowna, BC: Praxis (e) Press.
- Derudder, B., Devriendt, L., Van Nuffel, N., & Witlox, F. (2010). Geographies of business air travel in Europe. In J. V. Beaverstock, B. Derudder, J. Faulconbridge, & F. Witlox (Eds.), *International business travel in the global economy* (pp. 31–56). Abingdon, UK: Ashgate.
- Dodge, M., & Kitchin, R. (2004). Flying through code/space: The real virtuality of air travel. *Environment and Planning A*, 36, 195–211.
- Dodge, M., & Kitchin, R. (2006). Exposing the secret city: Urban exploration as 'space hacking'. Paper presented at the Association of American Geographers annual meeting, Chicago, IL.
- Dolen, M. (2011). US Mint ends the dollar coin 'scam' for airline miles (<http://www.businessinsider.com/us-mint-ends-the-dollar-coin-scam-for-airline-miles-2011-7>) Accessed 29 February 2016.
- Edmonston, P. (2009). AMR gets \$2.9 billion in new liquidity. *New York Times* 17 September <http://dealbook.nytimes.com/2009/09/17/american-airlines-gets-29-billion-lifeline/> Accessed 13 February 2016.
- Flyertalk. (2006). Swiss Knights Fondue and Cheese purchase for AA miles master thread. (<http://www.flyertalk.com/forum/american-airlines-aad-vantage-pre-consolidation-closed-posting/623306-swiss-knights-fondue-cheese-purchase-aa-miles-master-thread.html>) Accessed 24 February 2016.
- Flyertalk. (2009). US Mint dollar coin FAQ. (<http://www.flyertalk.com/forum/milesbuzz/1008566-us-mint-dollar-coin-faq-please-read-before-posting-coin-thread.html>) Accessed 29 February 2016.
- Ford, H., & Graham, M. (2016). Provenance, power, and place: Linked data and opaque digital geographies. *Environment and Planning D: Society and Space*, <https://doi.org/10.1177/0263775816668857>
- FrequentMiler. (2013). Million mile madness: Final tally. (<http://frequentmiler.boardingarea.com/tag/million-mile-madness/>) Accessed 13 February 2016.
- FrequentMiler. (2016). Credit card spend in 2016 and beyond. (<http://frequentmiler.boardingarea.com/2016/01/07/manufacturing-spend-in-2016-and-beyond/>) Accessed 29 February 2016.
- Fuchs, M., Fizek, S., Ruffino, P., & Schrape, N. (2015). *Rethinking gamification* (p. 344). Lüneburg: Meson Press.
- Garrett, B. (2013). *Explore everything: Place-hacking the city*. New York, NY: Verso Books.
- Garrett, B., Moss, A., & Cadman, S. (2016). *London rising: Illicit photos from the city's heights*. Prestel: Random House.
- Graham, S. (1998). The end of geography or the explosion of place? Conceptualizing space, place and information technology. *Progress in Human Geography*, 22, 165–185.
- Graham, S. D. (2005). Software-sorted geographies. *Progress in Human Geography*, 29, 562–580.
- Graham, M., De Sabbata, S., & Zook, M. A. (2015). Towards a study of information geographies: (Im)mutable augmentations and a mapping of the geographies of information. *Geo: Geography and Environment*, 2, 88–105.
- Graham, S., & Marvin, S. (2001). *Splintering urbanism*. New York, NY: Routledge.
- Graham, M., Zook, M., & Boulton, A. (2013). Augmented reality in urban places: Contested content and the duplicity of code. *Transactions of the Institute of British Geographers*, 38, 464–479.
- Greenfield, A. (2013). *Against the smart city: A pamphlet*. New York, NY: Do projects.
- Hepworth, M. (1989) *Geography of the information economy*. London, UK: Guilford Press.
- Hillis, K. (1998). On the margins: The invisibility of communications in geography. *Progress in Human Geography*, 22, 543–566.
- Jordan, T. (2008). *Hacking: Digital media and technological determinism*. London, UK: Wiley.
- Kitchin, R. M. (1998). Towards geographies of cyberspace. *Progress in Human Geography*, 22, 385–406.
- Kitchin, R., & Dodge, M. (2005). Code and the transduction of space. *Annals of the Association of American Geographers*, 95, 162–180.
- Kitchin, R., & Dodge, M. (2011). *Code/space: Software and everyday life*. Cambridge, MA: MIT Press.
- Kiva. (2016). Lending teams. (<https://www.kiva.org/teams>) Accessed 29 February 2016.
- Latour, B. (1987). *Science in action: How to follow scientists and engineers through society*. Cambridge, MA: Harvard University Press.
- Lefebvre, H. (1968). *Le droit à la ville*. Paris: Anthropos.
- Leff, G. (2013). Answering reader questions: The mystery surrounding 'fuel dumps'. (<http://viewfromthewing.boardingarea.com/2013/01/29/answering-reader-questions-the-mystery-surrounding-fuel-dumps/>) Accessed 8 February 2016.
- Leff, G. (2014a). The Supreme Court Limited your right to sue a frequent flyer program: What it means to you. (<http://viewfromthewing.boardingarea.com/2014/04/03/supreme-court-limited-right-frequent-flyer-program-means/>) Accessed 30 January 2017.
- Leff, G. (2014b). American reveals its frequent flyer program data to the SEC: Here's what we learn. (<http://viewfromthewing.boardingarea.com/2014/08/10/americans-internal-frequent-flyer-program-data-reveals-truth-program/>) Accessed 13 February 2016.
- Leff, G. (2015). DOT will no longer make airlines honor mistake fares. (<http://viewfromthewing.boardingarea.com/2015/05/10/dot-will-no-longer-make-airlines-honor-mistake-fares/>) Accessed 8 February 2016.
- Lessig, L. (1999). *Code: And other laws of cyberspace*. ReadHowYouWant.com.

- Levy, S. (1984). *Hackers: Heroes of the computer revolution* (vol. 4). New York, NY: Doubleday Books.
- Lin, W. (2014). Flying through ash clouds: Improvising aeromobilities in Singapore and Australasia. *Mobilities*, 9, 220–237.
- Massey, D. (1991). A global sense of place. *Marxism Today*, 35, 24–29.
- Massey, D. (2005). *For space*. London, UK: Sage.
- Mitchell, W. J. (1996). *City of bits: Space, place, and the infobahn*. Cambridge, MA: MIT Press.
- Mott, C., & Roberts, S. M. (2014). Not everyone has (the) balls: Urban exploration and the persistence of masculinist geography. *Antipode*, 46, 229–245.
- Mr Pickles. (2011). How to quickly meet your minimum spend at no cost to you. 5 May (<https://web.archive.org/web/20120319174546/http://www.thempickles.com/blog1/?p=69>) Accessed 29 February 2016.
- Phillips, D. (nd). The proof is in the pudding. (<http://www.flyertalk.com/pudding.htm>) Accessed 24 February 2016.
- Reddit. (2016). Introduction to manufactured spending. ([https://www.reddit.com/r/churning/comments/3vqpwx/introduction\\_to\\_manufactured\\_spending/](https://www.reddit.com/r/churning/comments/3vqpwx/introduction_to_manufactured_spending/)) Accessed 29 February 2016.
- Reidenberg, J. (1998). Lex informatica: The formulation of information policy rules through technology. *Texas Law Review*, 7, 6.
- Schlappig, B. (2013). How to plan a US Airways 90,000 mile award from the US to Asia via Europe. (<http://onemileatime.boardingarea.com/2013/01/10/how-to-plan-a-us-airways-90000-mile-award-from-the-us-to-asia-via-europe/>) Accessed 12 January 2017.
- Schlappig, B. (2014). Cheap first class fares out of Colombo, Sri Lanka?. (<http://onemileatime.boardingarea.com/2014/10/14/cheap-first-class-fares-colombo-sri-lanka/>) Accessed 12 January 2017.
- Shaw, J., & Graham, M. (2017). An informational right to the city? Code, content, control, and the urbanization of information. *Antipode*. <https://doi.org/10.1111/anti.12312>
- The Economist. (2005). Frequent-flyer miles in terminal decline? *The Economist*, 6 January (<http://www.economist.com/node/3536178>) Accessed 27 January 2016.
- The Economist. (2013). Fuel dumping. Around the world in cheaper ways. *The Economist*, 19 November (<http://www.economist.com/blogs/guliver/2013/11/fuel-dumping>) Accessed 29 January 2016.
- Thrift, N., & French, S. (2002). The automatic production of space. *Transactions of the Institute of British Geographers*, 27, 309–335.
- Woodyer, T. (2012) Ludic geographies: Not merely child's play. *Geography Compass*, 66, 313–326.
- Zook, M. A. (2000). The web of production: The economic geography of commercial Internet content production in the United States. *Environment and Planning A*, 32, 411–426.
- Zook, M. A., & Graham, M. (2007a). The creative reconstruction of the Internet: Google and the privatization of cyberspace and DigiPlace. *Geoforum*, 38, 1322–1343.
- Zook, M. A., & Graham, M. (2007b). Mapping DigiPlace: Geocoded Internet data and the representation of place. *Environment and Planning B: Planning and Design*, 34, 466–482.
- Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, 30, 75–89.

**How to cite this article:** Zook M, Graham M. Hacking code/space: Confounding the code of global capitalism. *Trans Inst Br Geogr*. 2018;43:390–404. <https://doi.org/10.1111/tran.12228>