Bugging Out: Darknets as Parasites of Large-scale Media Objects

NB: This is an pre-proofed version of an essay accepted for publication in Media, Culture, and Society

Robert W. Gehl and Fenwick McKelvey

Abstract

Platforms and infrastructures have quickly become seminal concepts to understand large-scale computational systems. The difference between a platform and an infrastructure is subject to debate. In this paper, we use the concept of the darknet to describe how infrastructure tends toward being public with other things where platforms tend to private relations. The darknet reveals these relations negatively, as we discuss, by turning these media objects into that which they desire not to be. We analyze these negative relations through the concept of the parasite developed by Michel Serres. Through following how darknets parasite both platforms and infrastructure, we suggest a need to develop new concepts to understand the diversity of relations now possible in a network society.

Introduction

Parasites have always been part of computing. JCR Licklider, a key thinker and funder of early computing and networking, used the idea of symbiosis to describe a new paradigm of human-computer interaction (Waldrop, 2002). Humans and computer should be like

> The [fig] tree and the insect, [and] thus heavily interdependent: the tree cannot reproduce without the insect; the insect cannot eat without the tree (Licklider, 1960: 4)

Through the metaphor, Licklider proposed a new, more personal relationship to computing, thus affecting how we view these machines. Licklider's optimism about human-computer relations, however, required he neglect a few details about the insect's relation to the fig. The female wasp dies in the fig, breaking off its wings and antennae during entry. Only the larvae escapes, consuming the fig in the process and leaving the fruit's husk as the mother's tomb. By extension, human-computer interaction is not merely a symbiotic relationship of mutual aid, but a matter of power, exploitation, and

inequity. This lesson is important as attend to the growing ubiquity of computing in everyday life, made possible by large-scale systems that we have come to call infrastructures and platforms.

The concept of the parasite reminds us to attend to the changing, unequal, and downright weird relations that constitute modern computing. In this paper, we use the concept of the parasite to unpack the relationality of "infrastructures" and "platforms." To do so, we use a sort of parasite to these large-scale media objects, darknets. These hidden, often anonymous networks re-purpose infrastructures and platforms. Our paper begins with existing conceptualizations of platforms and infrastructures, emphasizing the observed distinction between the privateness of platforms and the publicness of infrastructure. We then turn to Serres's enigmatic theory of communication and relations to analyze platforms and infrastructures through their relation to darknets. We will provide a definition of darknets drawn from our empirical investigation into Freenet, Tor, and I2P. The heart of the paper is an examination of darknets in relation to other entities, where we reveal that, from one perspective, darknets are platforms, and from another, they are infrastructures. The key to this perspectival approach is the relationality of parasitism. We will then turn to ways in which other entities parasitize darknets, showing how struggles of dominance, decay, and taking-without-giving continue to morph darknets from platform to infrastructure and back again. Ultimately, we hope that digital media studies might appreciate its uncomfortable relationship with parasites.

The Negative Shapes of Infrastructures and Platforms

Relationality is one way to define platforms and infrastructures as concepts of large-scale media objects. Plantin el. al (2016) suggest that both concepts refer to the “relation between components.” In one sense, these concepts attend to the endogenous *material* relations of media systems – how they express an internal order – whereas these concepts also imply exogenous relations that allow platforms and infrastructures to connect to other systems. The electrical grid, as infrastructure, uses plugs to connect appliances, whereas Facebook, as a platform, uses its applications to connect third-party apps to its features. In these examples, we note that infrastructures tend toward relations based on standards,

while platforms depend on application programming interfaces.

Given the many ways to understand relationality – as technologies, social relations, or systems of value – we probe the conceptual differences between platforms and infrastructures through their relations with others, through their exogenous relations. In this paper, we suggest that platforms tend toward privatized relations with other things while infrastructures tend toward public relations with other things. Such a distinction roughly maps to the historical differences between infrastructures like the electrical grid and the highways systems as the epitome of modernist state interventions and platforms as a postmodern pastiche of similar products arranged in a marketplace accessible by private interfaces (Plantin et al., 2016). This distinction appears today in calls to nationalize large technology firms, a nostalgic call premised on retreating from the neoliberal, privatized turn and restoring public infrastructure (Srnicek, 2017).

We propose to investigate these tendencies in a novel way, by looking at their publicness and privateness through their oppositions. Following the example of Finn Brunton, we propose to consider infrastructures and platforms through a negative term, considering how a negative shape co-constitutes the object under analysis. In his book on undesirable online messages or spam, Brunton argues that “attention, the scare resource of human notice, is what makes a community on a network” and that these communities can be understood through what they are not. Spam “is the negative shape of the history of people gathering on computer networks” (Brunton, 2015: xvi). Here, then, we take up Michel Serres's parasite as a way to expand this sense of the negative shape. His book, *The Parasite*, rethinks fields such as information theory, communication, media studies, and science and technology studies and suggests that all social interactions are, at their core, parasitic (Serres, 1982). For Serres, "parasite" has three meanings: an entity that lives within a host (the most common connotation); noise, interruption, or static; and an (unwanted) guest at a table. Our immediate reaction might be to chase each of these things out, to remove parasites from hosts, to quiet noise, or to ask the unwanted guest to leave. Removing these seemingly interfering elements out might appear to make biological, communicative, or social relations much smoother.

Looking at what a system *desires not to be* might seem counter-intuitive; however, parasites are *essential* to understand any given system, especially how it changes or is in flux through its relations. As Stephen D. Brown sums Serres's thinking up,

> Serres inverts our usual sense of what is meant by communication, by displaying that it is noise and interruption which are fundamental to organising social relations.... In its place, he substitutes a framework where the vagaries of what occurs between speakers, as messages become diffused, subjected to inteference, scrambled and translated, become the source of the rich texture of social relations (Brown, 2004: 384).

In other words, Serres focuses our attention on interference, scrambling, taking-without-giving – simply put, parasitism – arguing that these do not interrupt or deny the operation of a system; rather, they are the very things *necessary* for systems to work at all.

Moreover, drawing on Serres, both Pasquinelli (2008) and Kokelman (2010) have pointed to an advantage of parasite theory: it is a ternary, rather than binary, model (Serres, 1982: 19). Rather than binary conceptions (noise/signal, communication/disconnection), the parasite concept urges us to consider third terms, such as channels, translators, mediators, and interlopers. Returning to Brunton (2015), his object of analysis is spam and its negative relation to online community. The threat of spam allows online community to define and perform its boundaries of dialog and conduct, even falling apart when the community can no longer keep up and everything ends up being spam. As Brunton shows, online communities, require a third term – the spam filter. Hence, the model becomes ternary: community/spam filter/spam.

We use the phenomenon of dark nets to explore how platforms and infrastructures try and fail to become respectively private or public as well as to look to look at the other accidents that occur in between. In the following section, we explore how darknets function in this parasitic, third-term role, specifically as they relate to the public Internet and private online platforms. Returning to our initial definition of the platforms and infrastructures we suggest that:

- darknets parasitize the Internet’s infrastructure to create private domains; and
- darknets parasitize platforms to create public networks of common bits and bandwidth.

But, in keeping with Serres’ emphasis on continual struggle, rot, and decay, we recognize that what

comes after the parasite is always another parasite. After reflecting on darknets, platforms, and infrastructure, we explore the ways the parasite might cause us to expand our vocabulary of relations online, including in relation to darknet-parasites themselves.

Darknets Definition

Darknets are computer networks which require special software to access. They use end-to-end encryption, thus securing connections from one machine to another. In addition, darknets use network protocols to direct traffic in such a way as to dissociate users' identities from their reading and publishing practices, thus anonymizing their users. As Bancroft and Reid explain,

> The darknet is the set of relay systems and encryption protocols that disguise the origin, destination and/or the content of internet traffic.... The darknet is... a way of using internet networks that allow for anonymous [information] hosting and communication (Bancroft and Reid, 2017: 500).

Or, as Aked defines it,

> Darknets are encrypted data networks that ensure data transmitted cannot be intercepted, changed, observed or read by an unauthorised party…. Darknets sit on 'top' of the Internet, in an encrypted cloud that cannot be viewed without the required software (Aked, 2011: 10).

We focus primarily on three darknets: Tor, the Invisible Internet Project (I2P), and Freenet, which are the most popular systems (Moore and Rid, 2016: 15). In all three cases, accessing these networks requires special routing software. To access Tor, I2P, or Freenet networks, one needs their respective routing software packages installed. After installing this software, the user must modify applications such as Web browsers (or use pre-configured browsers, such as the Tor browser) to route their network connections through the special software.

Once this software is installed and applications are configured, users can access digital services that cannot be accessed any other way, or they can host a digital service (for example, a blog or an email service) that can only be accessed by others using the same software (Gehl, 2018). Moreover, users of these systems are anonymized.

To illustrate the distinction between darknets and the Internet, take the example of web

browsing. Visiting a website on I2P, such as the hidden social networking site visibility.i2p, is quite different from visiting a standard website, such as Facebook.com, in that neither the visitor to visibility.i2p nor the operator of that site knows each others' real identities. The visitor's IP address and browser user agent string are obfuscated, making identifying the visitor extremely difficult. Likewise, the exact physical location of visibility.i2p is obscured. Couple this with end-to-end encryption and the result is networks that protect readers and publishers from corporate or even state surveillance by dissociating their browsing and publishing from their actual identities.

The adjective "dark" may bring to mind illegal or immoral activity. Indeed, journalist Jamie Bartlett's book *The Dark Net: Inside the Digital Underworld* (2014) and the Showtime/The Movie Network series *Dark Net* emphasize this connotation by essentially defining "darknet" as "anything bad that happens online," focusing on trolls, pornographers, child abusers, and hackers. Our definition of darknet, however, emphasizes its technical aspects, focusing instead on access, protocols, encryption, and network topologies. In this sense, our definition is more akin to "going dark" in communications – that is, moving communication away from clear and open channels and into hidden and encrypted ones. Ours is not an *a priori* normative judgment of what people use darknets for. This is not to say that bad activities cannot occur on darknets – indeed, as we will discuss below, they certainly do – but it gives us the advantage of not simply condemning darknets from the outset, nor indulging in a technological determinist perspective that assumes that encryption and anonymization will inherently result in reprehensible activities. Instead, our focus on technical features is in keeping with the traditions of media studies, infrastructure studies, and platform studies and allows us to consider darknets in parasitic relation to other infrastructures and platforms. We turn to this next.

Darknets Privatize Infrastructure

Because they encrypt and anonymize, darknets make public things private. In this sense, they appear to *parasitize public infrastructures to become more like private platforms.* Freenet, Tor, and I2P all rely on global Internet infrastructures. A concept used to understand this relationship is "overlay

network." As Hunsinger explains, "Darknets are securitized Internet networks operating *over* existing networks through encrypted traffic on those networks" (Hunsinger, 2015: 58 emphasis added. Also see Aked, 2011: 10). As overlay networks, darknets run at the upper (or application) layer of the Internet thereby depending on the Internet for many core functions all the while rhetorically and technically distinguishing themselves from the general Internet.

As networks that require special software to access, darknets take on some of the recognized dimensions of platforms: they are private and users opt in to them (Plantin et al., 2016: 7). They do not allow just any device or user to connect, only those with the proper software. They take on the now classic "walled garden" approach to communication, sequestering users from other networks. Moreover, darknets are generative like other programmable platforms (McKelvey, 2011). Freenet, Tor, and I2P invite programmers to extend and modify them as open source projects. As open source projects, they rely upon volunteer (and a few paid) coders to develop and maintain their various software modules. Beyond their programming, darknets invite new applications to be built on top of them, a key characteristics of platforms with their app ecologies. Early in its history, Freenet users developed jSite, a means to easily publish Web sites to Freenet, and Sone, a distributed microblogging system. I2P has seen additional applications such as Syndie, a distributed blogging system, and I2Psnark, a torrent system, built on top of it. A notable application built on Tor is Ricochet, an encrypted chat system.

But darknets do not turn just infrastructures into platforms as such; this triad requires reconsideration of each of the three terms and their relations. The parasite "invents something new... [and] builds a new logic" (Serres, 1982: 35). So what is the transformation caused by this darknet overlay and underlying Internet host? In the case of darknets, the new functions they privatize the Internet to create *anonymous communication* and *increased security of communication.* While other overlay networks abide by the Internet's unencrypted design (DeNardis, 2009), darknets turn the lights out, obscuring network traffic that was once in the clear. This is achieved through new virtual topologies overlaid on top of the old. In every way, the one-way arrow of the parasite, to borrow a

phrase from Serres, pierces the inner workings of the Internet's infrastructure. In doing so, denial of "real world" identities, authentication, and openness become the normal darknet operations (Gehl, 2017), even as these operations rely upon an underlying Internet which is increasingly invested in those very practices. And these logics extend to the applications built on top of them. Applications such as Freenet's social networking system Sone, I2P's blogging platform Syndie, and Tor's chat system Ricochet inherit this relationship between (platformic) parasite and (infrastructural) host: anonymous, encrypted applications built upon darknets riding upon the public Internet's underlying architecture. Parasites, for Serres, feast off the host in the dark.

Darknets' particular parisitivism can be readily seen in the one key element of the mainstream Internet: the public Domain Name System (DNS), where domain names (like www.google.com) are resolved to IP addresses. To developers of darknets, the public system is too open to abuse and needs to be replaced, to be privatized in a way. Ian Clarke, the founder of Freenet, argues that the public DNS gives too much power to centralized administrators and that it prevents Internet users from being anonymous (Clarke, 1999: 8). Freenet opts instead to use cryptographic keys for every file in its network. Likewise, both Tor and I2P have sought technical and administrative ways to avoid any of their traffic going to the public DNS (Gehl, 2018), opting instead to use their own private naming systems.

By eschewing the public DNS in favor of private addressing systems while at the same time parasiting the rest of the Internet infrastructure, Freenet, Tor hidden services, and I2P create new relationships between users and networks, information and authorship, platforms and infrastructures, and anonymity and identity in communication. Their avoidance of the public DNS in favor of private naming systems enables anonymous and private service hosting, but it is enabled in large part by the underlying public Internet infrastructure. These public infrastructures, at times, welcome these parasites. Tor and other darknets are proof of the generative capacity of the web, that its permissive protocols enable new uses and applications and foster innovation even at the expense of the infrastructure itself (Van Schewick, 2010; Zittrain, 2008).

Darknets Publicize Platforms

Looking at them from another perspective, darknets function as communication networks, linking hundreds of thousands of computers together to move data around the world. As distributed networks, we would argue they take on features of *public infrastructures through their parasitism of private platforms.* Specifically, darknets subvert property and ownership to create something approaching an information commons (Milberry and Anderson, 2009). The majority of Freenet, I2P, or Tor users install these programs to access these distributed networks; they donot relate to these systems as programmable platforms. In such cases where users install darknet software and then use them to access content, these systems fade into the background, becoming far less visible, sinking below the surface and facilitate access to information commons with fuzzy definitions of property and ownership, or what has been called the grey commons in piracy scholarship (McKelvey, 2015).

To be infrastructural, we argue, darknets parasite one of the earliest platforms: the personal computer. Scott Lash, in his foundational work on the concept, cites the Microsoft Windows Operating System, as his first example of a platform that enabled “participat[ion] in various kinds of technological life” (2002: 24). Historically the personal computer opposed the shared computing infrastructure or time-sharing and dumb terminal (Hu, 2015). Through the operating system as platform, users had access to a common computing environment *in a private wa*y, without sharing computer resources with anyone (unless today a virus parasites these resources to mine for a cryptocurrency or, in our case, start a darknet).

Darknets parasite the privatized platforms of operating systems in two ways: taking bits and taking bandwidth. Freenet takes bits. It stores data on the hard drives of those who run the system. Each installation of Freenet sets aside a folder on the user's hard drive where encrypted files are stored. As other peers request files, they are built from these data stores. The files on a user's computer have nothing to do with the user's own file requests: instead, they are randomly distributed across the network. There is no central storage of files; files are served from the users' computers. Freenet thus brings about a new relationship between user, computer, and network. In order to access the Freenet

infrastructure, users agree to allow Freenet to take up space on their computer platforms. Moreover, the user cannot access the files within the data store; the idea here is that they have "plausible deniability" about what their computer is storing (Toad, 2008). These files are stored based on their popularity; more commonly requested files are kept longer and in more encrypted data stores.

Both Tor and I2P parasite the personal computer as a circuit in a shared communication network. I2P, like Tor, relies on users' computers to act as peers, providing bandwidth to the network. Each peer acts as a router, and each router is linked together into "tunnels." As their technical documentation explains it, "I2P builds virtual 'tunnels' – temporary and unidirectional paths through a sequence of routers. These tunnels are classified as either inbound tunnels (where everything given to it goes towards the creator of the tunnel) or outbound tunnels (where the tunnel creator shoves messages away from them)" (*I2P: The Invisible Internet Project*, 2011). Every node takes part in these tunnels, providing the capacity for the network. For its part, Tor's parasitism relies on goodwill and voluntarism. As their Web site describes,

> The Tor network relies on volunteers to donate bandwidth. The more people who run relays, the faster the Tor network will be. If you have at least 2 megabits/s for both upload and download, please help out Tor by configuring your Tor to be a relay too (*The Tor Project*, n.d.).

Such relays come in four flavors: entry, middle, bridge, and exit. Entry relays help Tor clients enter the network. Middle relays carry traffic across the network. Bridge relays are like entry relays, except information about them is limited; the goal is to prevent governments from allowing Tor users access the network. Exit relays carry traffic out of Tor and into the regular Internet. Tor cannot function without relays, and thus it is reliant on the tens of thousands of volunteers who enable Tor to parasitize a portion of their private machines (Servers – Tor Metrics, n.d.).

Darknets thus impose a radical "making public" of our private platforms. When users install Freenet or I2P on computer platforms, these parasites turn host machines into nodes in their networks, storing or sending bits that the end user never explicitly approves of – indeed, may be largely unaware of – and yet must engage in in order to access the broader networks. We may be able to install darknet

software on our machines, we might be able to modify it, but if we want access to darknets as networks, we are required to give over a portion of our platforms to build the new infrastructure. This echoes Serres's repeated trope of the party, where the host's private home is taken over by (parasitic) guests – some invited, others not (Serres, 1982: 16). For a while, the private home becomes a public house.

What we learn as we think of the darknet/Internet parasite/host relationship is that darknets create new possibilities for communication as they enter into the parasitic relationship with infrastructures and platforms. We suggest that any studies of platforms and infrastructures consider their relationship as parasitic – not in a pejorative sense, but in Serres's sense – because this sheds new light not only on the distinctions and commonalities between these concepts, but also upon their relationality, the exchanges between them, and the transformations that arise due to parasitism. Darknets function as third terms among platforms and parasites, and they do so in a fascinating, slippery way – appearing to be platformic one moment by privatizing what was once public, then later publicizing the private and thus appearing to be infrastructural.

Chains of Parasites between Public and Private

Through the negative shape of darknets, we can better reflect on the particularities of their publicness of infrastructures and privateness of parasites. In one sense, the reaction to the darknets suggest that public infrastructures might welcome parasites while private platforms avoid them. Darknets to the internet as infrastructure legitimate the "generative web" just as darknets frustrate platforms as violations of the "acceptable usage policies." The negative shape helps to ascertain the positive desires of these large-scale media objects. Moreover, darknets also prompt a reaction from their hosts. We return to Brunton, who notes spam provokes *reactive publics* that are obliged to “be aware of the means of their own existence” in order to “manage themselves and their infrastructure” (Brunton, 2015: 9). In a similar sense, darknets help us identify the reactions of platform and infrastructure to their parasites that exemplify their specific tendencies. How do private platforms guard

against parasites who seek to exfiltrate their data? As much as these media systems invite us to study their *preferred*, smooth, neat relations, the parasite helps us to study the problematic, noisy, transformative relations that equally define these systems.

But just as media studies has troubled the boundary between public and private, the parasite helps us analyze those tertiary relations that come through platforms. What are the quasi-private, quasi-public systems that occur due to parasites? Darknets have created media systems that exist in between the platform and infrastructure, not quite public or private. As populizers of the term “darknet” warned, users access these networks to download previously privatized data, including intellectual property (Biddle et al., 2002). A popular use of Freenet, for example, is to share pirated content (MP3s and videos, for example). I2P also offers access to pirated content via torrents. Finally, a key justification for the development of Tor is its ability to protect whistleblowers and leakers – actors who publicize the internal workings of governments and corporations (Chertoff, 2017: 31). (This is not to mention all the pirated content, including stolen personal information, on Tor’s network). All of these activities might be decried as detrimental – but from another perspective, they are part of a larger infrastructure of dissent in the face of the increasing commodification of knowledge and securitization of government operations.

Parasitism also captures the trouble in finding a clear distinction between platforms and infrastructures because a large media system’s status as one or another depends on its relationship. The parasite helps us understand these relations to be in flux. Platforms and infrastructures can at once be privatizing and publicizing in their relations. Admittedly, this undermines a historical distinction between the two (where platforms succeed infrastructures), but such flux captures the potential of platforms to become infrastructures (and visa versa) – adding to the concerns about the platformization of the media infrastuctures. But more than a fork in the road, parasitism captures a networked society of interconnected platforms and infrastuctures parasiting each other. This move reflects one made by Serres: the production of "chains of parasites." Serres mathematically arranges parasites into chains, or perhaps better cascades, where one parasite is feasted upon by another, who in turn is feasted upon by

another ad infinitum. In addition, this is not a static structure, but a roiling, ever-changing one. Public and privates are kinds of relations in flux of the long parasitic chain that is the network society. Moreover, Serres argues that there is intense competition to be the "top" parasite, to be at the apex of the chain, where all resources inevitably flow. What happens when we start to follow these chains? What happens when we think of the larger systems that platforms and infrastructures find themselves in? Following Serres, we follow the chains of parasites into the lion's den.

The Lion's Den in Bluffdale, Utah

The arrow is an important image for Serres, since the arrowhead is a sort of triangle (recall that the parasite is a ternary concept). There are many arrows, Serres argues, and he recommends we follow them, even if they lead into a mighty parasite's mouth:

> All flows are oriented to [the wild den], and none come from it. All the footprints point toward the lion's den, but none come away... Oddly enough, here it is the spot of power, of absolute power, that of the lion, the king's place. But it is also a trap, an open maw (Serres, 1982: 26).

The disclosures of Edward Snowden had clearly drawn the line between the Internet's infrastructure and data surveillance by the major intelligence agencies of the United States, the United Kingdom, Canada, Australia and New Zealand. To paraphrase security researcher The Grugq (2012), these agencies are the "apex predators" of the Internet. Called the Five Eyes, these agencies gorge on the Internet's data through hidden rooms and cable splits embedded in data centers, carrier hotels and landing sites of submarine cables across the globe. The National Security Agency takes its lion's share of data back to its mega center in Bluffdale, Utah. Known as the Mission Data Repository (because Massive Data Repository sounded creepy) (Bamford, 2014), the NSA collects exabytes of data to store and process at a later day. It slurps up data just as it consumes energy and (more disturbingly) water from the high desert of Utah (Hogan, 2015). Here, we suspect the NSA collects even what it cannot know, storing away what it cannot eat for a later day.

The Five Eyes may be said to be the "top" parasite. Their success in building a global surveillance system has been to be the parasite of all things. This parasitic surveillance has succeed by

finding value in what others refuse: metadata. Depending on the communication theory, “the same substance stinks or smells wonderful” (Serres, 1982: 142). One person’s noise (or noisome smell) is another’s sweet signal. Even as they encrypt data and dissociate publisher/reader identities from what is published or read, darknets and parasites are not silent or even odorless. Encryption and anonymity is meaningful to those within the trusted network and meaningless to those outside it. For some, the anonymity to speak is sweet – "*stercus suum bene olet*" says Serres (1982: 144). In contrast, in a leaked document, the NSA claimed that “TOR stinks” and that the NSA could “never be able to de-anonymize all Tor users all the time” (Ball et al., 2013). The smell of Tor's onions (the nickname for its hidden Web sites) marks its private space. “The privatization of the common and the appropriation of space do not occur only by yelling or spitting; sometimes excrement is enough. The dog took a leak on its niche, where the philosopher would vomit” (Serres, 1982: 144). Tor smells to the NSA because it is so otherly, a kind of communication unsuitable to its decryption and analysis. But the NSA will collect its traffic nonetheless: it has the space in its server farm. The digital lion's den is massive and will consume all, even the foul-smelling, even the dark, and especially the nefarious. The NSA’s data center can be said to figuratively eat shit, collecting all those foul smelling darknets.

Parasitic data is generative. The lack of knowing likely motivates the NSA to collect data in the Mission Data Repository that it *could* one day make sense of, an *ex post facto* surveillance. That is perhaps the greatest way the intelligence agencies parasite darknets: they collect what they don’t currently know and can't currently understand. Reflecting obliquely on the Shannon model of communication, Serres notes that

> Communication theory is in charge of the system; it can break it down or let it function, depending on the signal. A parasite, physical, acoustic, informational, belonging to order and disorder, a new voice, an important one, in the contrapuntal matrix (Serres, 1982: 6).

Perhaps surveillance agencies might acquire a nose for onions. Javascript programs sniff for mouse clicks or browser fonts to de-anonymize and track users on Tor (Makrushin and Garnaeva, 2015; Shoemaker, 2016). The NSA had invested in quantum computing, hoping the new paradigm in computing would break all known forms of encryption (Rich and Gellman, 2014). These techniques –

the few publicly disclosed by this infamously private agency – illustrate the generative nature of the parasite: as darknets parasitize both the Internet and user's computers, and as parasites roam the darknets, state agencies – the lions – develop new techniques to control infrastructures and platforms.

In the end, we wonder if this is the site of our politics today. Where do these generative responses to the parasite manifest? How have the Five Eyes been authorized to be parasitic, to eat the lion's share, to consume the entire Internet infrastructure, not to mention significant shares of the power grid and water tables (Hogan, 2015)? The same might be said for corporate platforms (Facebook, Amazon, Apple, Google, Microsoft) whose machine learning and artificial intelligence programs are new paradigms to interpret and make sense of the noise of our digital traces, and who also eat material resources such as electricity, water, and human labor. So many arrows point to these maws, and it is by following them that we can interpret the relations of power today. Moreover, it is directly in relation to these maws, these all-seeing lion-parasites, that darknet network builders construct their systems in the first place (Gehl, 2018). The apex parasites beget parasitic darknets in an endless, roiling chain.

Parasites of Parasites

The lion is one animal Serres used to describe the parasite, one that helps understand what happens when we follow a parasitic chain. In thinking further about the parasite and large-scale media object, we may use some other metaphors to understand the kinds of possible relations beyond just public and private. Drawing on our first discussion of the fig and the wasp as well as provocations to use insects in media theory (Parikka, 2010), we suggest a few other parasites to extend our discussion of parasites, infrastructures, and platforms:

1. Idiobiont parasitoid

An idiobiont parasitoid prevent the further development of their hosts, redirecting blood and nutrients to grow their own distinct (*idios)* life (*biont)*. The fork of Tor exemplifies this parasitic relation. Serres's parasitic dinner guests may eat with forks, but darknets do not. The fork is often seen as a worst case

scenario for free software development. A fork happens when the code base and development splits into different factions. A fork is a true parasite, taking code without giving back. Tor, for instance, has had to fend off forks aimed at its codebase. As Free and Open Source Software (FOSS), Tor is licensed to allow others to modify its code, or even start a new project based upon the original code. Some developers tried to fork Tor amidst allegations of sexual assault and mismanagement of its board in 2016. The fork seems to have disappeared, but not without some details about its proposed design: ROTOR would have merged I2P functions into Tor, modifying the browser to support the other darknets' protocols and subsequently acting as an infrastructural gateway (Edwards et al., 2009) between those competing networks. Reactions to the Tor/ROTOR fork included worries about the health of the host. Competing versions of Tor would diminish the number of hosts in either system, weakening the nodal redundancy important for its anonymity. The parasite could kill off the host.

The idiobiont parasitoid is the parasite to other parasites. What happens when we follow the chain to discover another parasite? Serres writes, “a parasite never nourishes its children. Otherwise it would be in the position of host. A parasite defends itself from being parasited” (Serres, 1982: 131). In the case of the eventually abandoned fork of Tor, we see the tension between conceptualizations of platforms and infrastructures. As a programmable platform with a FOSS license, theoretically Tor *ought* to be forked. Forks in FOSS theoretically strengthen the ecosystem of free software. FOSS is arguably built upon such parasitism, with certain licenses allowing for taking code and never giving back upstream. Indeed, this is another way private platforms might become public through multiplication: imagine if Facebook’s codebase were open and hence it could be forked. But when the fork affects an *infrastructure* by diluting the number of devices and channels available to a network, the idiobiont parasitism produces a danger of killing the host *and* the resulting parasite.

2. Entomopathogenic fungi

Darknets traffic in everything. Its parasitic relationship with the user’s computers injects all data. This indiscriminate data sharing is a purposeful aspect of darknet technoculture: as Tor explains, “we can't

build free and open source tools that protect journalists, human rights activists, and ordinary people around the world if we also control who uses those tools" (steph, 2017). The quote is part of the Tor project's official response to the reports that *The Daily Stormer,* a Nazi Web site, moved operations onto a Tor hidden service. As *Slate* reported, "Nazis, white supremacists, and the alt-right have become a lot less welcome on the web. So they're building their own" with Tor (Glaser, 2017). Tor isn't alone: all three darknets we discuss in this paper have dealt with the illiberal use of free speech.

The Daily Stormer and other online hate group's turn to darknets is a kind of entomopathogenic fungi. Anyone who has watched the *Planet Earth* documentary might be familiar with one kind, the *ophiocordyceps unilateralis*, more commonly called the zombie ant fungus. It infects the brains of camponotini ants, causing their host to climb from the forest floor to a leaf above where it attaches itself and waits for the fungus to grow. Like a flower from a seed, the fungus eventually ruptures the ant's head. A spore pod grows above the carcass then blooms to be spread by the breeze of the jungle canopy. The fungus, as a whole, sharply deviates from the ant's own interests, suggesting that one parasitic effect might be relations that mis-appropriate a platform or infrastructure. Like the zombie fungus, the overt project of white racial purity infects darknets designed without content moderation. Free speech absolutism can be a deadly parasite for the dark. Building on McKelvey (2015), darknets are a kind of centrifugal communication, fleeing from a centre and authority of moderation. The spores of online extremism infect this project, using the elusive design of darknets to create unmoderated content.

Darknets have to adapt, find new ways to avoid being parasitized. There is no criterion for what the data are: it could be legal or illegal data. Freenet developers frame the parasitization of user computers in terms of public, infrastructural community signal and noise: if the Freenet peer-to-peer users do not like particular classes of content, they need to chase out this content with good content. Freenet users concerned about illegal content are told to push more legal (or respectable) content into the network and to promote it, the idea being the "good" content will drown out the "bad." In other words, like Serres on the telephone at the feast (Serres, 1982: 67), Freenet developers tell their users to

cross a threshold, to push bad content away as noise and increase good content as messages. In doing so, they replicate the free speech absolutists' adage: bad speech must be chased out with good speech.

3. Cymothoid Isopods

The Cymothoa exigua plays a trick on its host, the fish. It disguises itself as a tongue after eating the host's original. Other cymothoid isopods consume and replace other organs of their hosts. These jokers have an ambivalent effect. The fish seem to get along fine with the new tongue. In following the parasitic chain one last time, we find that in the end that the thresholds between host, parasite and something else become easily confused. As we know, some darknets prevent users from knowing the content on their computers, but some darknets confuse all content. I2P relies on its peer to provide "cover traffic." As I2P's "Gentle Introduction" puts it,

> I2P's intent is to allow people to communicate in arbitrarily hostile environments by providing good anonymity, mixed in with sufficient cover traffic provided by the activity of people who require less anonymity. This way, some users can avoid detection by a very powerful adversary, while others will try to evade a weaker entity, *all on the same network*, where each one's messages are essentially indistinguishable from the others (*I2P: The Invisible Internet Project*, n.d.).

In other words, as they build tunnels and shunt data to and fro, each user's computer platform provides noise to the infrastructure, thus making traffic of interest (say, the communications of political dissidents) harder to find. The theory behind "cover traffic" or encrypted files in data stores on darknets is the theory of the joker, a wild card that is, depending upon the context, signal or noise. The joker, a particular kind of parasite, is a wild card for Serres. He writes,

> The noise is a joker. It has at least two values, like the third man: a value of destruction and a value of construction. It must be included and excluded (Serres, 1982: 67).

In following this parasitic chain one last time, all we have is static. We can imagine a government agent asking: is this traffic or file a signal of interest, perhaps that of a dissident? Or is it another cat video, or just a fake tongue? Again, parasitization brings about new relations: between individual's private computers, public flows on infrastructures, noise, signal, and surveillance. Once again, our analysis of darknets shows the fluidity of concepts such as infrastructure and platform. Looking at darknets

through the lens of the parasites shows that darkents can be public, private, *or* neither public, nor private.

Conclusion

By taking up Serres's parasite, we attend to relations: between platform and infrastructure, infrastructure and platform, public and private, user and machine, networks and noise, and states and encryption. And we attend to third terms. We do so in the hopes that others find Serres's relational approach useful for the study of digital media and communications. In light of platformic and infrastructural parasites, we echo Matteo Pasquinelli's caution against digitalism: "After depicting the 'information revolution' as a truly emancipatory movement for decades, it is quite difficult to acknowledge its parasitic side" (2008: 61).

The parasite, in this paper, has first helped us distinguish between the publicness of infrastructures, the privateness of platforms and the sum of parasitic chains in this novel take on a media ecology. When we relate to infrastructures, platforms, and above all each other, we have to move past static, fixed models of communication to dynamic, roiling, and disturbing patterns, acknowledging parasitism, the making public of what was once private or the privatization of the commons.

Darknets has helped us capture the variance between being public and being private as they themselves can be both. Darknets are platforms when we need them to be: we can program them, modify them, extend them, all to evade the lions. Or they become infrastructures when we need them to be: extending out across the globe, shunting deterritorialized data from one state territory to another, routing around censorship as the old saying goes. The desire to chase out the parasitic darknets brings about new developments in darknet technology as the networks and the lions struggle for control.

These parasites are a part of large-scale media objects. As the Internet’s core infrastructure intensifies powerful actors' moderation of content, surveillance of user activities, and control of daily, digitally-mediated life, darknets provide an outlet, an escape route, a different way of thinking. Would the much-discussed corporate enclosure (Andrejevic, 2007) of the public Internet be untenable without

an outside, an uncontrolled space? Could we stomach clean, neat, moderated, and policed network infrastructures without at least a few platforms that provide outlets for messes, outbursts, anonymity, and anomie? Even if we recoil at what we see, we must recognize that growth and change are only possible when parasites are present. We cannot simply chase them out. As Serres warns us: "The return of the grasshoppers..., the return of the excluded, the return of the repressed... will never stop" (Serres, 1982: 97).

References

Aked S (2011) An investigation into darknets and the content available via anonymous peer-to-peer file sharing. In: 2011. Available at: http://ro.ecu.edu.au/ism/106/ (accessed 22 June 2015).

Andrejevic M (2007) Surveillance in the digital enclosure. *The Communication Review* 10: 295–317.

Ball J, Schneier B and Greenwald G (2013) NSA and GCHQ target Tor network that protects anonymity of web users. *The Guardian*, 4 October. Available at: http://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption (accessed 26 September 2017).

Bamford J (2014) Edward Snowden: The Untold Story. Available at: https://www.wired.com/2014/08/edward-snowden/ (accessed 27 September 2017).

Bancroft A and Reid PS (2017) Challenging the techno-politics of anonymity: the case of cryptomarket users. *Information, Communication & Society* 20(4): 497–512. DOI: 10.1080/1369118X.2016.1187643.

Bartlett J (2014) *The dark net: inside the digital underworld*. London: Windmill Books.

Biddle P, England P, Peinado M, et al. (2002) The darknet and the future of content protection. In: *ACM Workshop on Digital Rights Management*, 2002, pp. 155–176. Springer.

Brown SD (2004) Parasite logic. *Journal of Organizational Change Management* 17(4): 383–395. DOI: 10.1108/09534810410545137.

Brunton F (2015) *Spam: A Shadow History of the Internet*. Cambridge, Mass.: MIT Press Ltd.

Chertoff M (2017) A public policy perspective of the Dark Web. *Journal of Cyber Policy* 2(1): 26–38. DOI: 10.1080/23738871.2017.1298643.

Clarke I (1999) *A distributed decentralised information storage and retrieval system*. Master's thesis, University of Edinburgh. Available at: http://www.decuslib.com/DECUS/vmslt00a/net/freenet.pdf (accessed 22 June 2015).

DeNardis L (2009) *Protocol Politics: The Globalization of Internet Governance*. Cambridge: MIT Press.

Edwards PN, Bowker GC, Jackson SJ, et al. (2009) Introduction: an agenda for infrastructure studies. *Journal of the Association for Information Systems* 10(5): 6.

Gehl RW (2017) Proactive Paranoia. Available at: http://reallifemag.com (accessed 24 August 2017).

Gehl RW (2018) *Weaving the Dark Web: Legitimacy on Freenet, Tor, and I2P*. Information Society. Cambridge, MA: MIT Press.

Glaser A (2017) Nazis and White Supremacists Are No Longer Welcome on the Internet. So They're Building Their Own. Available at: https://slate.com/technology/2017/08/the-alt-right-wants-to-build-its-own-internet.html (accessed 26 September 2017).

Hogan M (2015) Data flows and water woes: The Utah Data Center. *Big Data & Society* 2(2): 2053951715592429. DOI: 10.1177/2053951715592429.

Hu T-H (2015) *A prehistory of the cloud*. Cambridge, Massachusetts: The MIT Press.

Hunsinger J (2015) Produsing the hidden: darknet consummativities. In: Lind RA (ed.) *Produsing theory in a digital world 2.0*. New York: Peter Lang, pp. 57–73.

I2P: The Invisible Internet Project (2011) Tunnel Routing. Available at: https://geti2p.net/en/docs/how/tunnel-routing (accessed 13 September 2017).

I2P: The Invisible Internet Project (n.d.) A Gentle Introduction to How I2P Works. Available at: https://geti2p.net/en/docs/how/intro (accessed 13 September 2017).

Kockelman P (2010) Enemies, Parasites, and Noise: How to Take Up Residence in a System Without Becoming a Term in It. *Journal of Linguistic Anthropology* 20(2): 406–421. DOI: 10.1111/j.1548-1395.2010.01077.x.

Lash S (2002) *Critique of Information*. Thousand Oaks: SAGE Publications.

Licklider JCR (1960) Man-Computer Symbiosis. *Human Factors in Electronics, IRE Transactions on* HFE-1(1): 4–11.

Makrushin D and Garnaeva M (2015) Uncovering Tor users: where anonymity ends in the Darknet. Available at: https://securelist.com/uncovering-tor-users-where-anonymity-ends-in-the-darknet/70673/ (accessed 26 September 2017).

McKelvey F (2011) A Programmable Platform? Drupal, Modularity, and the Future of the Web. *Fibreculture* (18). Available at: http://eighteen.fibreculturejournal.org/2011/10/09/fcj-128-programmable-platform-drupal-modularity-and-the-future-of-the-web/ (accessed 5 November 2013).

McKelvey F (2015) We like copies, just don't let the others fool you: the paradox of the Pirate Bay. *Television & New Media* 16(8): 734–750.

Milberry K and Anderson S (2009) Open Sourcing Our Way to an Online Commons: Contesting Corporate Impermeability in the New Media Ecology. *Journal of Communication Inquiry* 33(4): 393–412.

Moore D and Rid T (2016) Cryptopolitik and the Darknet. *Survival* 58(1): 7–38. DOI: 10.1080/00396338.2016.1142085.

Parikka J (2010) *Insect Media: An Archaeology of Animals and Technology*. Minneapolis: University of Minnesota Press.

Pasquinelli M (2008) *Animal spirits: a bestiary of the commons*. Rotterdam, The Netherlands; [Amsterdam]; New York, NY: NAi Publishers ; Institute of Network Cultures ; Available in North, South and Central America through D.A.P.

Plantin J-C, Lagoze C, Edwards PN, et al. (2016) Infrastructure studies meet platform studies in the age of Google and Facebook. *New Media & Society*: 1461444816661553.

Rich S and Gellman B (2014) NSA seeks to build quantum computer that could crack most types of encryption. *Washington Post*, 2 January. Available at: https://www.washingtonpost.com/world/national-security/nsa-seeks-to-build-quantum-computer-that-could-crack-most-types-of-encryption/2014/01/02/8fff297e-7195-11e3-8def-a33011492df2_story.html (accessed 27 September 2017).

Serres M (1982) *The parasite*. Baltimore: Johns Hopkins University Press.

Servers – Tor Metrics (n.d.). Available at: https://metrics.torproject.org/networksize.html (accessed 23 August 2017).

Shoemaker N (2016) Tor Users Can Be Tracked by Their Mouse Movements. Available at: http://bigthink.com/natalie-shoemaker/tor-users-can-be-tracked-by-their-mouse-movements (accessed 26 September 2017).

Srnicek N (2017) We need to nationalise Google, Facebook and Amazon. Here's why | Nick Srnicek. Available at: http://www.theguardian.com/commentisfree/2017/aug/30/nationalise-google-facebook-amazon-data-monopoly-platform-public-interest (accessed 26 March 2018).

steph (2017) The Tor Project Defends the Human Rights Racists Oppose. In: *Tor Blog*. Available at: https://blog.torproject.org/tor-project-defends-human-rights-racists-oppose (accessed 26 September 2017).

The Grugq (2012) OPSEC: Because Jail is for wuftpd. Available at: https://www.youtube.com/watch?v=9XaYdCdwiWU (accessed 19 December 2016).

The Tor Project (n.d.) Relay Configuration Instructions. Available at: https://www.torproject.org/docs/tor-doc-relay.html.en (accessed 13 September 2017).

Toad (2008) [freenet-support] update and more questions.

Van Schewick B (2010) *Internet Architecture and Innovation*. Cambridge: The MIT Press.

Waldrop MM (2002) *The Dream Machine: J.C.R. Licklider and the Revolution That Made Computing Personal*. New York: Penguin Books.

Zittrain J (2008) *The Future of the Internet and How to Stop It*. New Haven: Yale University Press.