Article

new media & society
1–17

DOI: 10.1177/1461444814554900
nms.sagepub.com
SAGE

Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network

Robert W Gehl
The University of Utah, USA

Abstract

This essay is an early ethnographic exploration of the Dark Web Social Network (DWSN), a social networking site only accessible to Web browsers equipped with The Onion Router. The central claim of this essay is that the DWSN is an experiment in power/freedom, an attempt to simultaneously trace, deploy, and overcome the historical conditions in which it finds itself: the generic constraints and affordances of social networking as they have been developed over the past decade by Facebook and Twitter, and the ideological constraints and affordances of public perceptions of the dark web, which hold that the dark web is useful for both taboo activities and freedom from state oppression. I trace the DWSN's experiment with power/freedom through three practices: anonymous/social networking, the banning of child pornography, and the productive aspects of techno-elitism. I then use these practices to specify particular forms of power/freedom on the DWSN.

Keywords

Dark web, freedom, power, social networking sites, The Onion Router

This essay is an early ethnographic exploration of the Dark Web Social Network (DWSN), a social networking site (SNS) only accessible to Web browsers equipped with The Onion Router (Tor). Whereas most research on social networking focuses on mainstream, corporate SNSs such as Twitter and Facebook, this essay is a contribution to scholarship on alternatives to such mainstream sites (e.g. Lovink and Rasch, 2013). My

Corresponding author:
Robert W Gehl, Department of Communication, The University of Utah, Salt Lake City, UT 84112, USA.
Email: robert.gehl@utah.edu

central claim is that any viable social networking alternative will be an experiment with both freedom and power. In other words, just as mainstream SNSs are marked by both power (in the form of surveillance, algorithmic regulation of user activities, and architectural constraints) and freedom (in the form of user-led production, political organization, and new forms of online sociality), so too will any alternative. To be an alternative, the specific mix of power/freedom in any social media alternative must be different from mainstream SNSs. This specificity needs to be analyzed empirically and then conceptualized. I argue that the DWSN is an experiment in power/freedom, an attempt to trace, deploy, and overcome the historical conditions in which it finds itself. These conditions include the generic constraints and affordances of social networking. Moreover, since the DWSN exists on the dark web, these conditions also include the ideological constraints and affordances of public perceptions of the dark web. The DWSN negotiates both of these historical threads.

This article is organized as follows. First, I offer a brief note on doing ethnography on the dark web, looking to a previous study for methodological guidance. I then explore the dominant media ideologies of the "dark web" in order to do two things: (1) lay out part of the historical and popular context the DWSN finds itself in and (2) find categorical lenses with which to look at the DWSN. Most journalistic work on the dark web presents it as composed of illicit activities in need of policing. Yet, this dominant conception is complicated by a secondary conception of the dark web as a site of radical freedom of speech. I will next use this double-bind to tease out how the DWSN functions within a tension between freedom and power. Finally, I theorize the specific mix of power/freedom found on the DWSN, arguing that the DWSN is engaged in experiments with anonymity and infrastructure. Ultimately, I hope to answer several questions: how does social networking on the dark web work? What does this tell us about contemporary SNSs, anonymity, and privacy? In what new ways do power and freedom intersect in an SNS that exists solely on the dark web?

Dark web ethnographic method

Because this is an ethnography of a dark web SNS, there were several methodological challenges. The dark web is different from the "clear web" in important ways. The dark web is part of the Internet that cannot be accessed by mainstream software.[1] It includes hidden sites that end in ".onion" or ".i2p" or other Top-Level Domain names only available through modified browsers or special software. Accessing I2P sites requires a special routing program. Accessing non-mainstream Top-Level Domains through OpenNIC requires the user to change the DNS server addresses on his or her router. Accessing .onion sites requires Tor (for a tutorial on Tor and .onions, see Hoffman (2012)).

Moreover, those who run dark websites that end in .onion are able to hide their identities and locations from most, if not all, Internet users (Dingledine et al., 2004). In most cases, a visitor to a .onion site will not know the identity of the host, nor will the host know the identity of the visitor. This is very different from the mainstream Internet, where sites are often associated with a company or location (e.g. google.com is associated with the company headquartered in Mountain View, CA), and visitors are often

identified and monitored through sundry tracking technologies such as cookies, account registrations, Flash cookies, IP addresses, and geolocation.

Although these technical conditions are challenging for ethnography, they are not unique in the ethnographic literature. In doing a participant observation of the DWSN, I followed the example of anthropologist Tom Boellstorff's (2008) ethnography of Second Life. Boellstorff takes Second Life on its own terms; he avoids linking Second Life avatars to their "real-world" counterparts in order to focus on day-to-day life in that virtual world. He treats Second Life as its own space, with its own rules and culture, rather than as articulated with the "real world" outside of the virtual. This is a methodological choice of Boellstorff's (Winnick, 2008), as opposed to the work of, for example, danah boyd (in press), who studies social media users both online and offline.

For me, however, I have no choice but to study the DWSN on its own terms. I cannot link DWSN avatars to their flesh-and-blood counterparts even if I wanted to. This is for the technical reasons I mention above, but also due to the culture of the DWSN. According to the DWSN privacy policy, "In order to protect everyone's privacy, you have to protect yourself. You can do this by not giving out any personal information. No personal emails. No real names. No specific location information." Due to this, I did not seek to learn any personal information from DWSN members (including name, age, gender, location). Moreover, due to an agreement I made with the members of the DWSN that I spoke to, all user pseudonyms have been made into new pseudonyms (i.e. "an admin" and "a member"). I did receive an exemption for this study from my university's Institutional Review Board (IRB). Most of this material is taken from public parts of the DWSN ("public" insofar as they are accessible with Tor and a DWSN account), with some material drawn from one-on-one interviews conducted through private messaging. These interviews were preceded with informed consent notices. In all cases, in keeping with my university's IRB standards, I offered to reveal my identity to those I interviewed, but (in keeping with the strictly anonymous character of the DWSN) my identity was refused. However, I also provided a draft of this essay to the DWSN administrators I spoke to and have revised according to their feedback (call it another round of blind peer review).

Thus, just as Boellstorff did with Second Life, I focused on how DWSN members interact within the site and how the site is structured. In this sense, I paid attention to the governance and interaction dynamics of the site in much the same manner as Geert Lovink's (2003) analyses of the Amsterdam Digital City and nettime (but without any offline contact with DWSN members). That is, I engaged in participant observation, focusing on the intersection between site architecture (Davis, 2010; Star, 1999) and member actions in the vein of digital ethnography as explicated by Gabriella Coleman (2010), paying attention to "various frames of analysis, … history, and the local contexts and lived experiences of digital media" (p. 488).

Power/freedom: lenses to see in the dark (web)

Although the strict anonymity of the DWSN narrowed the scope of my work (in that I could not talk to DWSN members offline), an ethnography of any SNS must also be focused. Despite being less accessible than "clear web" SNSs such as Facebook or Twitter, the DWSN has shown evidence of growth since its founding in 2013. During my

observation of the site over a period of 10 months, the DWSN's number of accounts grew from 3000 to over 24,000, with over 170 groups, hundreds of blog posts, and tens of thousands of micro-blog posts. Although these are not numbers on the scale of Facebook or Twitter, they are impressive, given that finding the DWSN is not a simple matter of Googling for it. More to the point, it would be impossible to observe or speak with thousands of people.

To focus my study, I sought lenses (or "categories," as Koopman and Matza (2013) would call them) with which to illuminate activities on the DWSN. The two I use are *power* and *freedom*. These lenses, I should stress, are not free-floating concepts that I will simply grab from a theoretician and then "apply" to the DWSN. These lenses come from the context in which the DWSN emerges: the "media ideology" (Gershon, 2010) of the dark web, specifically as this ideology appears in journalistic coverage. This coverage forms part of the historical context the DWSN finds itself operating in, and thus, journalists' articulation of "power" and "freedom" informs the experiments with power/freedom I explore in the DWSN below.

I see two main threads in news reporting about the dark web, with one dominant and the other less dominant but quite prevalent. First, there is the conception of the dark web as entirely composed of illegal or taboo activities and in need of policing. Second, there is the idea that the dark web can preserve a valued liberal freedom: freedom of speech. Thus, what appears in this media ideology is a "reciprocal and incompatible" (Foucault, 2006: 529; Koopman, 2013: 163) relationship between power and freedom.

The popular media coverage of the dark web is redolent of moral panics that have been associated with Internet culture over the past 35 years, such as the panic about computer hackers and phone phreaks in 1980s (resulting in the arrest of many young computer users); the US Congress' Communications Decency Act of 1996, brought on by a moral panic about pornography on the Web; and the US Congress Deleting Online Predators Act of 2006, inspired by moral panics over pedophiles on Myspace. Especially since the media coverage of the Silk Road drug market bust and the Freedom Hosting child pornography (CP) bust, both in 2013 (Borland, 2013), the dark web is currently inspiring similar panics centering on fears of CP, the drug and gun trade, and killers for hire.

One *Sun* headline is a series of adjectives that bind the dark web with CP: "Child sex dark web targeted" (Wooding, 2013). A reporter for *The Age* notes the dark web is "where pornographic images to satisfy the most depraved tastes can be downloaded" (Ormsby, 2012). The dark web is "a hub for black markets that sell or distribute drugs" (Pagliery, 2014). *Gizmodo* profiled the dark web gun store The Armory, asking "Could a band of anonymous weapon mongers prepare me and 19 imaginary compatriots for illegal warfare? If you've got a spare million or so, looks like the answer is yes" (Biddle, 2012). The *Daily Mail* calls Tor a "seething matrix of encrypted websites" where one could hire hitmen for US$10,000. "So for those looking to bump off a difficult acquaintance, all they have to do is enter the Deep Web—known also as the 'Dark Web' or the 'Undernet'—and search 'hitman for hire'" (*Mail Online*, 2013). Implicit throughout this coverage is a call for more policing of the dark web (e.g. Biddle, 2012; Bingham, 2013; Gillespie, 2013; Henry, 2013; Murad and Hines, 2012).

Despite this dominant idea of the dark web as only useful to pedophiles, assassins, and junkies, recently more Internet users have started to use Tor and even hidden .onion

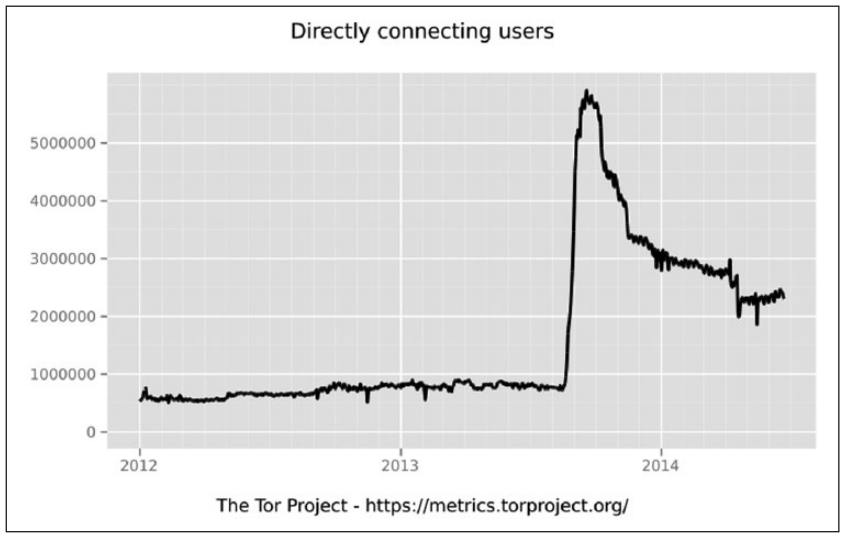

Figure 1. The rise in Tor users occurring between 2012 and 24 June 2014. The large spike has since been attributed to a Ukrainian botnet. However, after the spike, usage has clearly gone up. This is attributed to the Snowden revelations about the NSA.
NSA: National Security Agency; Tor: The Onion Router.

sites (see Figure 1). This rise has been attributed in part to Edward Snowden's revelations about National Security Agency (NSA) and General Communication Headquarters (GCHQ) surveillance of the Internet (Borland, 2013). For privacy purposes, this is a positive development; more Tor users means more traffic and thus more obfuscation of user identities (Dingledine et al., 2004). This ties in with a secondary thread in popular coverage of the dark web: its affordances for journalists, activists, and whistleblowers who want to speak freely, despite state monitoring of the Internet. Many of the above-cited stories note that anonymizing software such as Tor can benefit anyone who wants to dissociate speech from identity, including political dissidents (e.g. Pagliery, 2014). As *National Public Radio* reported,

> Tor's executive director is working with victims of domestic abuse who need to communicate without being tracked by their abusers. Tor is also used by Chinese dissidents who can't access sites like Twitter. And it became a valuable tool during the Arab Spring. (Rath, 2014)

Wired reports, "While not a perfect means of anonymity, [Tor] has become widely used by journalists communicating with sources, human rights activists, and dissidents in war-torn areas such as Syria" (Borland, 2013). As this secondary thread in the media ideology holds, Tor and hidden .onion sites can be used for free speech, a liberal ideal.

Thus, this media ideology portrays the the dark web as a place of excessive freedom (due to anonymity), which is in need of forms of power[2] to contain that excess. However, this ideology also posits a limit to power in the form of the liberal right to free speech.

Power and freedom are overdetermined here, and the devil is in the details as to what is protected speech and what is in need of policing. Admittedly, this reciprocal and incompatible power/freedom assemblage presented in journalistic coverage of the dark web is somewhat simplistic, but of course journalism can powerfully shape other discursive arenas (e.g. policymaking). Drawing on Wendy Chun's (2006) work on power and freedom on and through the Internet, the journalistic coverage of the dark web allows us to see how this reciprocal incompatible power/freedom relationship is *extramedial* to the dark web itself, representing it for curious people, causing the dark web to "exist within the public's imagination before" use of the dark web can become "a regular public practice" (p. 23). Such coverage constitutes a historical a priori to many users' confrontations with the dark web—myself included—and it has shaped and no doubt will continue to shape uses of the dark web. Here, following the examples of Chun and Foucault, I want to pick up these journalists' power/freedom lenses with an eye toward empirically finding and then conceptualizing specific, concrete forms of power/freedom I observed in the DWSN, a very particular use of the dark web. I turn to that observation next.

Three practices on the DWSN

The DWSN should be readily recognized as an SNS: it allows for individual accounts, with customizable member pages, connections through "friending," social praise in the form of "liking," and a Twitter-like micro-blogging system, among other features. As an SNS, there are generic and architectural constraints and affordances built into the software, and these are used by administrators and members to shape the site's culture. Like other SNSs, the DWSN has terms of service (TOS) and a privacy policy. These are enforced in a variety of ways, including through discussion and through technical measures like deleting of posts or member accounts. Finally, there are cultural norms that are expressed by both members and administrators as they communicate in the site.

All of these elements contribute to the DWSN's particular assemblage of reciprocal incompatible tensions of power/freedom. I illustrate this with three specific DWSN practices: the anonymous/social networking, the prohibition against CP, and the productive aspects of techno-elitism.

Anonymous/social networking

It is notable that the popular press coverage of the dark web explored above does not discuss SNSs. SNSs, it appears, are outside the media ideology of the dark web. For journalists covering the dark web, the idea of dark web users engaging in social networking in the generic forms we now recognize—for example, friending, following, liking, posting—seems to be unimaginable. That is, there is no articulation of "social networking" with either illicit activities or liberal free speech on the dark web.

This tells us something about the current social mediascape. Contemporary social networking, especially Facebook, is now associated with the use of real-world identities and is (perhaps because of this) considered to be a safe and acceptable online practice. Facebook specifically has been quite successful in fostering a culture of "real-world identities," but it did so in the face of a culture of anonymity and pseudonymity that was

prevalent on the Web from 1990 on. We can contrast Facebook, which was initially only open to those with a Harvard email address, with its mid-2000s rival Myspace, which allowed anyone with an email account to sign up. During their mid-2000s rivalry, Facebook grew as Myspace was mired in moral panics about fake accounts, pedophiles, and cyberbullying (Marwick, 2008). In contrast, Facebook users were vetted first by their university email accounts and later by their real-world social networks, and thus, Facebook was seen as "safer" for users (boyd, 2007) as well as advertisers (Gehl, 2012). This practice is continued to this day, as Facebook requires new users to verify their identity with a mobile phone account or a government-issued ID.

The DWSN is more redolent of social networking before Facebook, that is, social networking with pseudonyms. In fact, Facebook's aggressive mapping of real-world identities is part of the problem that the DWSN seeks to address. As the DWSN creator puts it, "[DWSN] was born in an impulse, I was deeply upset about facebook sharing/selling my personal data and with the general lack of privacy on the clear web." Whereas social networking prior to Facebook left it up to users to decide whether or not they wanted to use their "real-world" identities, Facebook's culture of real-world identities has made it extremely attractive to marketers who seek precision in their targeted advertising (Gehl, 2014). Moreover, users of Facebook have done the work of mapping their "social graphs," which allows governments to easily trace dissident and criminal networks (Semitsu, 2011).

In contrast, the DWSN privacy policy (excerpted above) asks that members reveal no personal information about themselves. Although this cultural norm helps produce the possibilities of anonymous speech, it comes with a price: *members must adhere to the policy*. Here, anonymity is not springing from liberal freedom, but is rather a cultural and technical requirement of the site itself. A key text in the DWSN mythology, Mentor's "Hacker Manifesto," illustrates this. Part of the "Manifesto" addresses identity:

> This is our world now … the world of the electron and the switch, the beauty of the baud …. We exist without skin color, without nationality, without religious bias … and you call us criminals …. Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like.

A copy of the "Manifesto" was posted to DWSN in April 2014 by a DWSN admin. In a discussion we had a few months later about identity on DWSN, this same admin cited the "Manifesto" and said,

> Tell me who you ARE not WHO you are. [DWSN] isn't all about anonymity, it's about soul. It's about putting a piece of yourself out there for the world to see that you otherwise would have been too hesitant to allow others to witness in a traditional setting.

This admin calls for disembodied communication dissociated from putatively superficial markers such as race or gender, evidenced by the idea of an essential "soul" that emerges through discourse. This is a longstanding ideal of the Internet, perhaps best illustrated by John Parry Barlow's (1996) "Declaration of the Independence of Cyberspace" (and best challenged, it should be noted, by the work of Lisa Nakamura (2002, 2007)).

During my time on the site, I have seen this policy reinforced largely through discussion. For example, an admin told me that if anyone does sign up for the DWSN with a real-world identity,

> We immediately contact them and help them understand their mistakes as fast as possible. We do not step in and change the account details, we're not nannies, we respect the idea that someone could do it purposefully but we step in to make sure the user knows what they are doing.

I have not seen anyone removed from the site for revealing personal information, but I also have not seen anyone reveal real-world names or email accounts. To do so would be, to use that administrator's term, a "mistake."

Moreover, this administrative enforcement appears to have affected the daily culture of the site. When one member used the DWSN blog to ask to meet others in the American Midwest in order to coordinate culture jams against various corporations, another member—not an admin—replied, "People spend time in Onionland because they are doing things that they want to keep hidden. Saying where they live, even a general area like the American Midwest, is rather counter to the point." After that, the original poster stopped discussing the American Midwest dark web networking idea. Here, the practice of not revealing personal information (i.e. one's physical location) is enforced through member-to-member discussion.

However, recent research has shown that online pseudonyms are very important to people who use them and that in fact much of the "real-world" identity of a user is manifested in an online persona (e.g. Gatson, 2011). Although the culture of the DWSN is premised on no personal information being revealed, thus freeing the member from telling others "WHO [they] are" as the admin I spoke to put it, the structure of social networking (with a stable, individual account, use of avatars, text-based self-descriptions, and accumulation of friends and accolades such as "likes") can mean that members invest much of their time—and thus their sense of self—into their DWSN pseudonyms, thus expressing "who [they] ARE."

This is important to emphasize: To engage in a practice of total anonymous freedom through the DWSN, one would have to create a new account every time one used the site, taking care never to link statements one makes to a coherent pseudonym. This is possible but is discouraged through the technical interfaces of the site as well as perceptions of how to "do" social networking. One does not use a fake account every time; one builds a *persona* (Gatson, 2011: 232; Marwick and boyd, 2010). This can be illustrated by considering member home pages on the DWSN, which feature textual descriptions of the member, avatars, and collections of "widgets" that the members can customize. It is also illustrated when members leave the site: often other members ask, "Where did X go?" Thus, although there is freedom in anonymity (a freedom enforced through policy and practice), there is also the cultural and technical constraints and affordances of social networking that mitigate against or delimit total anonymity. Anonymous/social networking is thus reciprocal and incompatible.

Returning to the dominant media ideology of the dark web, delinking real-world identity and online activity should immediately bring to mind the most common narrative

about anonymous online speech: that it is hateful, bent only toward the satisfaction of taboo or illegal desires. In this narrative, by (re)making social networking anonymous on the dark web, the DWSN should only be populated by terrorists and child pornographers, dark manifestations of liberal conceptions of freedom. However, here we can see another power/freedom tension play out, illustrated best by the problem of CP, a tension that adds another layer to the anonymous/social networking tension I have just laid out.

Surveillance in the DWSN: freedom from CP

Commercial activities (such as the trade of weapons and drugs) are not allowed on the DWSN, contradicting the popular conception of the dark web explored above. But above all, the site's biggest prohibition is against CP. According to an admin, child pornographers "are a problem on the dark/deep and we do not welcome them here …. CP is the true black sheep of the dark/deep communities." Another admin vowed, "I'll chase and ban all CP material." This is no easy task. To enforce this policy, administrators must constantly monitor the site; there are no technological solutions (such as filtering algorithms). An admin told me, "The tried and true way is for diligent admins to delete any user practicing this taboo immediately." However, this work gets reinforced as the culture of the site is defined in part as not allowing child pornographers: "Through this basic social filter we end up with a user base that primarily see the child pornographers as a problem as well and contributes to keeping an eye out for any potential abuses." Every page has a "Report This" button, and members are encouraged to use it if they see site violations.

Indeed, in my time on the DWSN, I have seen no evidence of CP or anything that might be defined as pornographic for that matter. I did witness one member asking for pictures of, specifically, 15-year-olds, but that member's post and account were deleted within a matter of minutes. Another asked for "kitty porn," perhaps as a way to defeat a potential filter against the phrase "kiddie porn"; that account, too, was deleted quickly. The DWSN's reputation as virulently anti-CP gets reflected in how it appears on the all-important link indexes of .onion sites—it is one of the few hidden SNSs listed by "No CP" indexes.

This is not to say that CP does not exist on the DWSN. It appears as a topic of political and ethical discussion. Many on the DWSN have discussed what to do about CP and pedophiles. The consensus, at least from my observation, is that heavy-handed laws and moral panics would do no good. The goals of the DWSN, which seem to be held by many members, are to maintain the technical and cultural capacities for anonymity and use the freedom associated with anonymous speech to challenge state and corporate power. As states propose or pass laws against CP, DWSN members often debate them. One example occurred after the BBC reported that downloading "child abuse manuals" was going to be made illegal in the United Kingdom, on a par with downloading manuals on how to be a terrorist (*BBC News*, 2014). DWSN members and administrators—many of whom who had in other places professed hatred of child pornographers—debated this move by the UK government. One member asked,

> What happens if someone is coerced into downloading such a manual, naively (e.g. tell them it's a crack for a video game, etc), then reported (anonymously of course) to the cops? What

> happens if someone genuinely accidentally downloads such a manual? What happens if someone's machine is compromised, then their HD filled with such manuals?

Another added,

> The annoying thing about this kind of law to me is it's pure gesture. This is going to do fuck all to stop children being sexually abused. Society's attitude toward pedophilia is very much brushing it under the carpet—making it more illegal, and never actually addressing the problem of pedophilia as a mental illness.

And another,

> I really hate CP and I think it should be fought [relentlessly;] however knowledge should never be illegal. First ban those manuals, then something else, then another thing then etc. and in the end only one book is legal in the country. That's the point.

Thus, although CP is banned on the DWSN, although members and administrators readily scour the site to remove any such material, members are vehemently against *states* banning the acquisition of CP-related materials. Notably, in the first quote, the member of this anonymous social network decried the use of *anonymity* to report an unwitting offender of this proposed law.

This is a complex mix of power/freedom, anonymity, and accountability, a mixture that is dangerous, where the right policy, technical infrastructure, and practice to deal with the serious problem of CP are never quite clear, but the consequences of laws and prohibitions can have devastating effects on populations. The DWSN, by banning CP and yet decrying that ban when states do it, is attempting to negotiate these incompatible and reciprocal practices.

Techno-elitism as community building

The apparent contradiction between residents of a DWSN decrying a state-based ban on CP while upholding their own ban within the architecture of their social network points us to another power/freedom tension: the productive aspects of techno-elitism. Many of the members of the DWSN use visible markers to show their technical proficiency: they discuss coding, hacking, and running pirate radio stations. This is redolent of the long-standing hacker culture of "do it yourself," which extends to governance: We do not need a clumsy state to regulate us; we can do it ourselves with superior information technologies (again, see Barlow's "Declaration" for a key text in this vein).

This techno-elitism appears in discourses about who is a proper DWSN member and who is not. Certainly, signing up for the DWSN is free, and within a few minutes, one can build a full profile and begin interacting with other members. On the face of it, the DWSN is very open and easy to use. However, given the fact that the site is hidden only to Tor users and moreover only to those who find the site (usually through .onion directories—themselves not always easy to find), technical knowledge is needed to join the DWSN. This technical knowledge is seen as a sort of "admissions test" one must pass before being seen as competent in helping build the DWSN community.

A discussion I had with an admin about the lack of popular media coverage of the DWSN reveals this techno-elitism. The admin I spoke to likened DWSN to a "corner cafe," a semi-private space that only locals know about. "Now one day you walk into your perfect corner of heaven to find some douchebag TV cooking show host standing in there with half a dozen cameras and a production team," the admin asks me to imagine. "Now your quiet little spot has been broadcast to every corner of the known globe." This would broadcast the cafe to people "too incompetent/lazy [to] find a place like it for themselves," effectively "watering down" the cafe. In this analogy, of course, DWSN is the cafe, and "douchebag TV cooking show" is "clear web" coverage of the site, which would attract too many users who were previously incapable of using Tor to find DWSN. Too many such "incompetent/lazy" people on the DWSN would harm the site's culture. As a member theorized, if the site becomes popular, "Ignorant users [would] flock to the DWSN and shitposting starts trending. The idyllic laid back administration system proves not enough and the site needs major structural changes to accommodate such a user base." Instead, both the admin and member argue for the site to remain hidden to anyone without the skills to use Tor and navigate hidden services. "Those with eyes to see can find us," the admin commented in a micro-blog post.[3]

This is illustrated well by the reaction to two "clear web" intrusions into DWSN. First was the discovery, early in the site's history, that Google was indexing DWSN, meaning that anyone doing a Google search could see content from the DWSN, even without a Tor-equipped browser. A DWSN admin called for a vote on whether to allow Google to continue indexing the site. Although the admin called for a vote, the admin somewhat shaped the discussion by noting, "even if [DWSN]'s objective is to provide a non-government, non-profit, anonymous dark web social network for citizens worldwide to share fruitful ideas, the fact that we can be seen [on Google search results] kinda sucks." Many users weighed in on the matter, arguing that Google should not be able to index anything on the DWSN. One member argued,

> I am here because I don't want to contribute to the likes of google and facebook. Allowing major entities to index the content here … will continue to have a significant chilling effect on what users will feel safe sharing here. Yes, [DWSN] is a "social network" but that doesn't mean we shouldn't value user privacy above all else …

Another member, who is also an administrator of another .onion site, noted,

> There is also the theory that "The teacher will appear when the student is ready." [New members] might make it to [DWSN] by google search but accessing the URL via TOR [requires] effort and in my opinion [is] the admission test.

In other words, having Google make any content from the DWSN appear on the "clear web" would make it too easy for novice users to discover the site. Installing Tor and finding the site's unique URL were presented as "admission tests."

A similar discussion occurred later when members posted to the site's micro-blogging feed (a 140-character feed similar to Twitter) that Wikipedia had an entry about the site. The Wikipedia entry, however, was subject to deletion because there are very few sources

to cite to prove the notability of the DWSN. Perhaps because the Wikipedia page was likely to be deleted, the discussion about it was somewhat more ambivalent than the Google discussion. One admin noted that the DWSN "is a living thing now, let's see what happens:)," implying that some "clear web" coverage might be tolerable. Another admin, however, bluntly stated "I'd prefer it just be deleted and disappear." A member expressed both views:

> i'm only here [since] a few days, need to find my way a bit and I think a bit more users to make [the DWSN] more "alive" would be cool … but with more coverage on the clearnet, who knows what kind of people start visiting.

Later, the Wikipedia entry was deleted, and one member quipped, "Awww. Maybe I should run over there and give [DWSN] a great writeup. NOT!"

These moments, probably more than anything else, illustrate how the DWSN administrators and members are experimenting with the incompatible and reciprocal power/freedom relationship. Through techno-elitism—that is, through the desire to keep the site hidden to those with the technological "eyes to see"—DWSN members and administrators establish a power relationship between themselves and those on the clear web: We are technical elites, and you are hapless clearwebbers caught in the nets of the NSA.

Moreover, the site is biased toward English. As one admin informed members,

> All [DWSN] texts will be in English as a primary and sole language. This means website text, policies, and notices sent by website admins, etc will always be in English. Other languages are welcomed and tolerated but they will not become official (or used by site staff) languages. Of course user created groups are welcome to use their own languages but [DWSN] was, is and will be a primarily English language site for the foreseeable future.

These practices—of being "in the know" and English-only policies—can be extremely exclusive and thus undermine the claims to "freedom" that permeate the site. After all, if NSA spying and Facebook surveillance are as terrible as many on the DWSN say they are, why not seek to get as many Internet users off the "clear web" and onto the dark web? Why not make the site accessible to non-English speakers?

However, such techno-elitism is not simply exclusive; it is productive. Maintaining the DWSN as a small community can aid in the shaping of the site culture as described above, allowing the administrators to police a smaller community for CP and other undesired practices and allowing the overall culture of the site to develop slowly over time. Requiring technical ability—the ability to install and use Tor, to find the site, and to sign up for an SNS without divulging personal details—is disciplinary, an encoding of particular actions and habits in potential site members, helping to *produce* the very subjects that the administrators want to enroll in the site. Similarly, making English an official language of the site excludes many people, but it is also the case that translating all site materials into other languages would likely require a massive amount of labor that the small number of administrators could not provide, distracting them from the work of cultivating the site.

These acts of power are productive and allow for particular forms of freedom. After passing those tests and agreeing to those cultural and technical constraints, users are free

to pursue many topics of discussion. There are groups discussing the continuing crises in Ukraine (in both Ukrainian and English), discussing protesting the Brazilian government's handling of the World Cup (with entries mainly in Portuguese), and discussing Spanish electoral politics (with entries mainly in Spanish). There are, unsurprisingly, groups dedicated to the cryptocurrency Bitcoin, information security, setting up and running .onion and.i2p sites, hacking (both in the "black hat" cracking sense and the "white hat" security research sense), filesharing, and drugs (although the sale of drugs on the site is forbidden per the TOS prohibition on commercial activity). But there are also groups for feminists, philosophers (although, seemingly, not *feminist* philosophers), archaeologists, labor rights activists, and news junkies. In other words, the DWSN is like many online gathering places: It is a teeming mix of many interests.

Conclusion: DWSN as an experiment with power/freedom

What do we make of these power/freedom tensions on the DWSN? As Foucault argues in "What is Enlightenment?," critique "is a historical investigation into the events that have led us to constitute ourselves and to recognize ourselves as subjects of what we are doing, thinking, saying" (Foucault, 1984: 45). Moreover, he argues, such critique must be about *experimenting* with such historically imposed limitations. The members and administrators of the DWSN are doing this critical work—tracing, deploying, and working against both the historical limits of mainstream social networking and the historical limits of the media ideology of the dark web. They know the dark web is seen in popular culture as only used by drug traders and child pornographers. They also know that mainstream social media—a "safe" space on the clear web—presents the problems of surveillance and the commodification of personal data. To experiment with both historical conditions, the DWSN is reverse engineering (Gehl, 2014) the functionality and cultural practices of sites such as Facebook and Twitter and porting these functions onto the dark web.

The DWSN is building a dark web space that is productive in two senses. First is the "be the media" sense of mainstream social media sites: the now-classic narrative about social media is that the user is in control and that all of us are "produsers" making our own culture through digital creativity (e.g. Bruns, 2008). However, the DWSN *is also* bringing software- and culturally developed social media *restrictions* to the dark web. In other words, it is porting in the standards of social media sites such as Facebook and Twitter: centralization, surveillance, prohibitions on actions, and the channeling user activity to algorithmic and interface-driven ends. Both of these interact in the heterogeneous assemblage, that is, the DWSN.

This brings me to the DWSN's specific assemblage of power/freedom. I am mindful of Foucault's (2008: 186) call to specify and concretize categories such as power and freedom, echoed by Coleman's (2010) call to "localize" and specify digital media (p. 489). Both Foucault and Coleman recommend empirical methods (i.e. genealogy, ethnography) to trace contexts and assemblages and avoid narrowing of any object *qua* universalizing it (see also Koopman, 2013).

In this vein, I would offer that the specific, concrete power/freedom practices of the DWSN center on *practices of anonymity* and *infrastructure*. Although at first glance

anonymity might simply appear to be a form of freedom and infrastructure simply a form of power, they are reciprocal and incompatible in that each contains elements of each. That is, there are moments we can speak of "anonymity-power": for example, the disciplinary admonitions to be anonymous on the DWSN, as well as the advantages of using a pseudonym to administer a site. We can also speak of "infrastructural-freedom": the mix of the infrastructure of existing .onion hidden services as well as open-source social media software packages to allow for a complex form of dark web communication and social expression that cannot exist on the "clear web." Moreover, this form of infrastructure-freedom is available to all who learn how to navigate it; it is a freedom that comes from the technical skill needed to find the DWSN.

We can of course speak of anonymity-freedom: the use of anonymous communication to explore ideas that are marginalized in more mainstream contexts, including proverbial "third rail" issues like suicide, violent political change, or pedophilia. As one DWSN member told me, if "I want to talk about things illegal in my country or report some abuse I can without fear of retaliation. This is it. Nothing exceptional." And we can speak of infrastructure-power: after all, the administrators can delete posts or accounts with relative impunity due to the centralization of the DWSN (I have witnessed this many times).

I see the DWSN as an experiment with power and freedom through anonymity and infrastructure, an experiment of going beyond historically imposed limits. In terms of social networking, the anonymous elements of the DWSN are a far cry from what we now would recognize as mainstream social media, which involves real-world identities increasingly linked to consumer preferences and noopolitical control (Gehl, 2013). Rather, the DWSN is not-for-profit and thus is not interested in producing its members as niche audiences to be sold to marketers. Moreover, the DWSN appears to be—although I cannot ever say for certain—virulently dedicated to protecting members against law enforcement and state power, something that cannot be said of Facebook, which after all has *patented a means to hand user data over to governments* (United States Patent, 2013).

Additionally, the DWSN is also dedicated to fighting the dominant conception of the dark web as a place that only the vilest among us want to be. Rather than fleeing the ever-supervised, ever-controlled Internet to some hidden, carefree corner where total anonymous freedom takes control, the DWSN shapes internal discourses in order to develop itself as (as its About page puts it) "a safe and moderated environment for the productive exchange of information." This is not a free-for-all, but neither is it a space where everything is controlled and thus happy (as Facebook seemingly wants to be).

The point is power and freedom *always* operate on one another. To challenge surveillance power as found in corporate social media and in state surveillance agencies and to challenge the ideology of an anything-goes dark web, the DWSN deploys an assemblage of anonymity and infrastructure to create an experimental "space-time" beyond the historical conditions it finds itself in (Deleuze, 1995: 172). Power and freedom "must be deployed simultaneously so that we can work within the internal tensions of their relationships" (Koopman, 2013: 169). To transform one, we have to transform the other in experiments. Such "experimental freedom perhaps does not make for good cinema on the blockbuster model. But it does make, and may make further, for good practices of

freedom" (Koopman, 2013: 174). The quiet, hidden, clear web-leery DWSN is just such an experiment, one that its members and administrators are always tinkering with—sometimes well, sometimes poorly, and never with guarantees. As Wendy Chun (2006) argues in *Control and Freedom*, "From our position of vulnerability, we must seize a freedom that always moves beyond our control, that carries with it no guarantees but rather constantly engenders decisions to be made and actions to perform" (p. 30).

Acknowledgements

The author would like to thank Colin Koopman, Jessica R. Houf, the anonymous reviewers, and especially the members of the DWSN for their comments and feedback on this project.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Notes

1. The "dark web" is also often referred to as the "deep web," but journalists and technologists who discuss the dark web take pains to distinguish the two. The "deep web" is defined as all the material online that commercial search engines such as Google and Bing cannot access (Bergman, 2001). This includes databases, information behind login barriers, and automatically generated content that only appears online for brief periods. This content is not indexed by search engines, but it still can be reached with a standard browser (e.g. a stock installation of Firefox). This is distinct from the "dark web," which requires special software to access.
2. The specific form of power that journalists call for is not quite clear. It could be what Foucault called discipline, what Deleuze called control, what Lazzarato or Neidich called noopower, or what Galloway called protocol. Or it could take another shape, perhaps a mix of other forms across multiple national and local contexts. Tracing the specific contours of the assemblage of surveillance, manipulation, and punishment that would be needed to "clean up" the dark web is the subject of another study.
3. Although the administrators and members of the DWSN are wary of popular coverage of their social network, those that I spoke with were welcoming of my pursuing an academic publication. But because of their concern about "clear web" coverage, I ultimately decided to keep the real name of the site redacted.

References

Barlow JP (1996) *A Declaration of the Independence of Cyberspace*. Available at: https://projects.eff.org/~barlow/Declaration-Final.html

BBC News (2014) Law to target child abuse "manuals," 27 April. Available at: http://www.bbc.com/news/uk-politics-27177040

Bergman MK (2001) *The Deep Web: Surfacing Hidden Value*. Available at: http://bright-planet.com/wp-content/uploads/2012/03/12550176481-deepwebwhitepaper1.pdf

Biddle S (2012) The secret online weapons store that'll sell anyone anything. *Gizmodo*, 19 July. Available at: http://gizmodo.com/5927379/the-secret-online-weapons-store-thatll-sell-anyone-anything

Bingham J (2013) Cameron wins FBI support for "dark web" war on paedophiles. *Daily Telegraph*, 2 November, p. 2.

Boellstorff T (2008) *Coming of Age in Second Life: An Anthropologist Explores the Virtually Human*. Princeton, NJ: Princeton University Press.
Borland J (2013) For tor, publicity a mixed blessing. *Wired*, 28 December. Available at: http://www.wired.com/2013/12/tor-publicity-mixed-blessing/
boyd d (2007) Viewing American class divisions through Facebook and MySpace. Available at: http://www.danah.org/papers/essays/ClassDivisions.html
boyd d (in press) Making sense of teen life: strategies for capturing ethnographic data in a networked era. In: Hargittai E and Sandvig C (eds) *Digital Research Confidential: The Secrets of Studying Behavior Online*. Cambridge, MA: MIT Press.
Bruns A (2008) *Blogs, Wikipedia, Second Life, and Beyond: From Production to Produsage*. New York: Peter Lang.
Chun WHK (2006) *Control and Freedom: Power and Paranoia in the Age of Fiber Optics*. Cambridge, MA: MIT Press.
Coleman EG (2010) Ethnographic approaches to digital media. *Annual Review of Anthropology* 39(1): 487–505.
Davis J (2010) Architecture of the personal interactive homepage: constructing the self through MySpace. *New Media & Society* 12(7): 1103–1119.
Deleuze G (1995) *Negotiations: 1972–1990* (trans. M Joughin). New York: Columbia University Press.
Dingledine R, Mathewson N and Syverson P (2004) *Tor: The Second-Generation Onion Router*. Available at: http://dl.acm.org/citation.cfm?id=1251396
Foucault M (1984) What is enlightenment? In: Rabinow P (ed.) *The Foucault Reader*. New York: Pantheon Books, pp. 32–50.
Foucault M (2006) *History of Madness* (trans. J Murphy; ed. J Khalfa). New York: Routledge.
Foucault M (2008) *The Birth of Biopolitics: Lectures at the Collège de France, 1978–79* (trans. M Senellart). New York: Palgrave Macmillan.
Gatson SN (2011) Self-naming practices on the Internet: identity, authenticity, and community. *Cultural Studies↔Critical Methodologies* 11(3): 224–235.
Gehl RW (2012) Real (software) abstractions: on the rise of Facebook and the fall of MySpace. *Social Text* 30(2): 99–119.
Gehl RW (2013) What's on your mind? Social media monopolies and noopower. *First Monday* 18(3–4). Available at: http://firstmonday.org/article/view/4618/3421
Gehl RW (2014) *Reverse Engineering Social Media: Software, Culture, and Political Economy in New Media Capitalism*. Philadelphia, PA: Temple University Press.
Gershon I (2010) *The Breakup 2.0*. Ithaca, NY: Cornell University Press.
Gillespie I (2013) Cyber cops probe the deep web. *The Age*, 24 October, p. 11.
Henry R (2013) Inside the murky world of the deep web. *The Sunday Times*, 2 June, p. 19.
Hoffman C (2012) How to find active onion sites and why you might want to. In: MakeUseOf. Available at: http://www.makeuseof.com/tag/find-active-onion-sites/
Koopman C (2013) *Genealogy as Critique: Foucault and the Problems of Modernity*. Bloomington, IN: Indiana University Press.
Koopman C and Matza T (2013) Putting Foucault to work: analytic and concept in Foucaultian inquiry. *Critical Inquiry* 39(4): 817–840.
Lovink G (2003) *Dark Fiber: Tracking Critical Internet Culture*. Cambridge, MA: MIT Press.
Lovink G and Rasch M (eds) (2013) *Unlike Us Reader: Social Media Monopolies and their Alternatives*. Amsterdam: Institute of Network Cultures.
Mail Online (2013) The disturbing world of the Deep Web, where contract killers and drug dealers ply their trade on the Internet, 11 October. Available at: http://www.dailymail.co.uk/news/

article-2454735/The-disturbing-world-Deep-Web-contract-killers-drug-dealers-ply-trade-internet.html
Marwick AE (2008) To catch a predator? The MySpace moral panic. *First Monday* 13(6). Available at: http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2152/1966
Marwick AE and boyd d (2010) I Tweet honestly, I Tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media & Society* 13(1): 114–133.
Murad A and Hines N (2012) Drugs, guns and passports for sale on "Dark Web." *The Times*, 3 April, p. 12.
Nakamura L (2002) *Cybertypes: Race, Ethnicity, and Identity on the Internet*. New York: Routledge.
Nakamura L (2007) *Digitizing Race: Visual Cultures of the Internet*. Minneapolis, MN: University of Minnesota Press.
Ormsby E (2012) The net's underbelly. *The Age*, 1 June, p. 13.
Pagliery J (2014) The Deep Web you don't know about. *CNN Wire*, 10 March. Available at http://money.cnn.com/2014/03/10/technology/deep-web/
Rath A (2014) Going dark: the Internet behind the Internet. *NPR, Weekend All Things Considered*, 25 May. Available at http://www.npr.org/blogs/alltechconsidered/2014/05/25/315821415/going-dark-the-internet-behind-the-internet
Semitsu JP (2011) From Facebook to mug shot: how the dearth of social networking privacy rights revolutionized online government surveillance. *Pace Law Review* 31: 291.
Star SL (1999) The ethnography of infrastructure. *American Behavioral Scientist* 43(3): 377–391.
United States Patent (2013) *Automated writ response system*. Patent 8438181, USA, 7 May. Available at: http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.htm&r=1&f=G&l=50&s1=8,438,181.PN.&OS=PN/8,438,181&RS=PN/8,438,181
Winnick D (2008) On coming of age in second life: an interview with Tom Boellstorff. *Anthropology News* 49(7): 21.
Wooding D (2013) Child sex dark web targeted. *The Sun*, 15 September, p. 24.

Author biography

Robert W Gehl is an assistant professor in the Department of Communication at The University of Utah. His first book is *Reverse Engineering Social Media* (2014, Temple).