Routledge
Taylor & Francis Group

Continuum

Journal of Media & Cultural Studies

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/ccon20

Dark web advertising: the dark magic system on tor hidden service search engines

Robert W. Gehl

To cite this article: Robert W. Gehl (2021): Dark web advertising: the dark magic system on tor hidden service search engines, Continuum, DOI: 10.1080/10304312.2021.1983251

To link to this article: https://doi.org/10.1080/10304312.2021.1983251

Published online: 07 Oct 2021.

CONTINUUM: JOURNAL OF MEDIA & CULTURAL STUDIES
https://doi.org/10.1080/10304312.2021.1983251

Routledge
Taylor & Francis Group

OPEN ACCESS

Dark web advertising: the dark magic system on tor hidden service search engines

Robert W. Gehl

Communication and Media Studies, Louisiana Tech University, Ruston, USA

ABSTRACT

Drawing on Raymond William's concept of the 'magic system,' this article argues that advertising on the Dark Web is a 'dark magic system'. The article first defines 'Dark Web' and then analyzes over 300 banner advertisements appearing on Tor onion service search engines. The advertisements are categorized into navigation, individual vendors, services, and markets. Next, the article traces the associations the advertisements make between advertised objects and values. The predominant values the advertisements invoke include navigation, OPSEC politics, and a justification to exploit the openness of others. The article then traces the limits of the dark magic system, including the system's inability to offer metrics, the problems of 'onion cloners,' and the constant threat of scams. The article concludes with an argument that the dark magic system is incapable of addressing the sort of anonymized political communication the Dark Web might afford.

KEYWORDS

Dark web; advertising; tor; raymond williams; search engines

Introduction

Raymond Williams's essay 'Advertising: The Magic System' initially appeared in *The New Left Review* in 1960 and has since been heavily anthologized as a cultural studies classic (Williams 1960, 1993, 2000). Drawing on Marx's provocative concept of the commodity fetish, Williams argued that advertising's function is to create associations between the objects being sold and subjective values. Williams's commitment to socialism (Williams 1993, 410) prompted him to argue that the promised associations of the 'magic system' always fall short of social needs:

> If the consumption of individual goods leaves that whole area of human need unsatisfied, the attempt is made, by magic, to associate this consumption with human desires to which it has no real reference. You do not only buy an object: you buy social respect, discrimination, health, beauty, success, and power to control your environment (Williams 2000).

Despite appearing over 60 years ago, Williams's condemnation of the emptiness of the magic system seems more relevant today than ever. This is because the magical associations Williams mapped in his essay – beer with manliness, a washing machine with social

CONTACT Robert W. Gehl ✉ rgehl@latech.edu
Robert W. Gehl is the F. Jay Taylor Endowed Research Chair of Communication at Louisiana Tech, and is the author of *Weaving the Dark Web* (MIT Press, 2018).

proof of status – are only intensified and reified in contemporary online advertising, particularly within corporate social media, such as the properties owned by Facebook (Facebook, WhatsApp, Instagram)or Alphabet (the whole Google suite).

While we're on what I will call in this essay the 'Clear Web,' we are subject to monitoring by corporations (Fuchs 2012). We are constantly profiled, our tastes mapped, our desires fitted into psychographic categorization systems (Stark 2018). These elements of our online activities are filtered, sorted, and fed back to us. Lest each of us think that we are alone, corporate social media assures us we're not: our friends like this product, too. Our families love visiting this tourist spot. The influencers we follow recommend this shampoo. We can join in the magic, too, liking, sharing, and posting about our own transfigurations and transmutations through consumption. Thanks to ubiquitous online surveillance, our *belief* in the magic can be mapped. As we search for, purchase, rate, and talk about products through social media, advertisers and marketers gain a deeper understanding about which magical associations work for whom and how well. All the while, the surveillance-driven magic appears to get more and more fantastical, more *real*, as its practitioners learn more and more about us.

Dark web advertising's dark magic

I want to keep this discussion of the magic system of Clear Web advertising in mind as I turn to the object of this paper: the peculiar practices of *Dark Web* advertising, specifically on general purpose search engines that index Tor hidden services. I am interested in the production and circulation of advertisements happening on encrypted, anonymizing networks, which are very different contexts than the corporate-dominated Clear Web. Riffing off of Williams, I suggest that Dark Web advertising is a 'dark magic system.' Thinking of it this way requires me to trace the implied associations that Dark Web advertising is making. But my extensive, ethnographic experience studying both Dark Web and Clear Web advertising practices (Gehl 2016, 2018) also allows for me to conceptualize the particular relationship Dark Web advertising has with Clear Web practices.

First, however, I should clarify some terms. I define the 'Dark Web' as comprised of:

> websites built with standard web technologies (HTML, CSS, server-side scripting languages, hosting software) that can be viewed with a standard web browser, such as Firefox or Chrome, which is routed through special routing software packages . . . . The major differentiating factor between the Dark Web and the Clear Web is that these special routing systems are designed to provide anonymity for both visitors to websites and publishers of these sites (Gehl 2018, 8).

Tor, the most popular Dark Web system, features *onion sites*, websites which a) are only accessible via Tor and b) anonymize *both* the reader of the website *as well as* the publisher of the site.[1] Tor onion sites largely look like the regular web: we see them through a web browser, they are built with HTML and other web languages. They have text, images, links, and URLs. However, unlike the Clear Web, they are 'dark' in the sense that they anonymize both readers and producers of content.

Note that this is not a moral definition. I am not using the term 'dark' to describe the *content* of Dark Web sites – I'm focusing on the technical structure of systems like Tor. Certainly, there are unethical, exploitative, prurient, and vicious sites on the Dark Web, but there are such sites across the entire Internet.

As a system using standard web technologies, the Dark Web includes familiar types of websites: search engines, blogs, forums, and wikis. Within many of these there are Web-style advertisements, predominantly banner advertisements appearing on search engines and to a lesser extent on social media. Such advertisements are my focus.

Approach to studying advertising on tor search engines

Here, I draw on several years of ethnographic observation of Dark Web advertising practices, particularly on Tor onion sites (Gehl 2016, 2018), and couple that experience with a systematic review of 320 banner advertisements posted across 24 general-purpose search engines (i.e. search engines claiming to both have crawled all Tor hidden services and be able return accurate search results). I analyse a snapshot of current Tor search engine advertising through the conceptual lenses I developed during my ethnographic analysis of the Dark Web.

Many Tor users have established search engines which offer search results based on their indexes of onion sites. I have been observing these search engines since 2014, and focused a chapter of my book on them (Gehl 2018, chap. 5). The search engines appropriate much of the look and feel of Google – search bar, text results, and very often, advertisements paid for by third parties. While I have observed Dark Web-based advertising in multiple places, one consistent location for such advertisements is on general-purpose search engines, such as Torch, TorDex, or Submarine. Not all search engines sell advertising space – notable here are Ahmia and Not Evil.

Because the Dark Web anonymizes readers and creators of content, when advertisements appear on general-purpose search engines, they are not personalized. They can't use cookies, logins, or IP address tracking. In fact, if the search engines used these tactics, they would likely be shunned by users – the Dark Web is designed to mitigate these tracking technologies. Thus, the advertisements I see will be the same as what you see if you were to look at the precise same time as me. Moreover, Dark Web search engine advertising has been stable over the past few years: I have not observed much churn in the advertisements over the years, especially in terms of the categories I will discuss below. Advertisements for directories and single vendors appear today much as they did during the early days of my research. The advertisements I collected in March of 2021 are comparable to the screenshots of the search engines I have collected over the past half decade.

The 320 advertisements were collected over a period of several consecutive days as a snapshot of search engine advertising. I did not examine speciality search engines, such as ones that focus on drug markets (e.g. Recon). Search engines – general or otherwise – are not the only places where Dark Web advertisements can be found. I should also note that some of the search engines I looked at are likely 'clones,' meaning that they are essentially fraudulent versions of an original search engine – I will discuss this issue below. Rather than remove them from the collection as duplicates, I think it's important to trace the relationships between possibly cloned engines and advertisements and the original engines and advertisements.

Williams (1960) used a variety of approaches to study the magic system, including historical analysis, political economic analysis, categorization of advertisements into types, and above all, tracing the associations the advertisements create between product and fantasy. In the interest of space, I will emulate the latter two, categorization and tracing associations. For both purposes, I visited the sites being advertised (although I have not bought anything on the Dark Web).

Because the users of the Dark Web are anonymized, we have little insight into their identities. The Dark Web is not amenable to gathering any sort of demographic information. However, Williams's orientation to the associational, semiotic nature of advertising helps us here – we can consider the magical associations that Dark Web advertisements are making and infer the values of the audience the advertisers are imagining. Moreover, because the Dark Web has been developed in part as a reaction to the surveillance practices of the Clear Web, we can also conceptualize the dark magic system's product offerings as part of that reaction.

Categories of dark web advertisements

A large proportion of the advertisements are for *navigational sites*: lists of links, directories, and even other search engines. One third of the advertisements I collected fall into this category. They reflect the fact that Tor onions are hard to navigate, even with a search engine. There are many advertisements for sites such as the 'Hidden Wiki,' 'Tor Links,' or 'Onion Links | Verified & Safe.' Clicking through, we see collections of ostensibly vetted links of onion sites the user can visit, in categories such as blogs, forums, image boards, markets, and porn sites. Twenty of these navigational sites explicitly advertise themselves as anti-scam lists, offering lists of identified scam sites or verified, trusted sites.

These somewhat dull advertisements for navigational sites compete with more exciting offers, including advertisements for *individual vendors*, small shops selling products. A third of the advertisements I collected fall into this category. A common advertisement is 'BUY REAL MONEY' on a garish yellow background with stacks of green money on either side. Clicking through, we're invited to 'Change your Life NOW!!!'. This Dark Web site offers to sell real money, including Euros, GBP, USD, Swiss Francs. The vendor claims they have access to actual currency marked for destruction at various central banks. Other vendors offer stolen credit card information, prescription drugs, or hard narcotics. No matter the product, nearly every individual vendor claims to be the most trusted, most reliable purveyor of the goods – or your money back.

A related category is for *services*, people who are selling their skills rather than a product. One eye-catching advertisement asks: 'your wife are cheating you?' [sic]. If so, the advertisement suggests that '[you] Get in control. Hire a hacker.' Indeed, many hacker services are advertised across the Dark Web, claiming to be able to hack into social media accounts, recover lost passwords, exfiltrate corporate or government secrets, or, as this particular advertisement promises, monitor one's wife. Another advertisement, the 'Porn Hacker,' offers to hack into paid porn accounts. This advertisement features animated GIFs of actual pornography – predominantly nude women – and promises access to premium pornography sites like Brazzers, LiveJasmin, Pornhub, and Chaturbate. Several advertisements offer an escrow service to aid in commerce. And perhaps the most infamous service advertised on the Dark Web is the 'hitman for hire' service – there are several banner advertisements offering that service.

But individual vendors and service providers often gather at *multi-vendor markets*, another common advertisement category. There's a lot of competition between markets, and so there's a lot of attention-seeking in their advertisements. One advertisement I've seen many times during my years exploring the Dark Web is an animated gif of a pair of jiggling breasts in a tank top, alternating with the phrase 'HIDDEN MARKETPLACE' and images of USD and Euro signs. Clicking through, we find the Hidden Marketplace has vendors offering credit cards, fake money, money transfers, gift cards, gadgets, and 'Porn and Erotic' products. The bulk of their products, it appears, are monetary: presumably stolen credit information or counterfeit monies. Other markets specialize in drugs, and some claim to sell weapons.

The remaining advertisements in the collection fall outside these broad categories. There are advertisements for stolen bitcoin wallets, cryptocurrency multipliers that promise to double your Bitcoins, gold bullion, hidden social media and forums, fixed football matches, and, interestingly enough, advertisements selling advertising space on other sites. They often use flashing gifs, nude women, and close-up shots of money to catch the eye.

Dark magic associations

Based on my categorization and analysis of search engine-based advertisements, I argue that there are three key associations happening between the advertisements and larger, networked practices, forming a dark magic incantation:

> *navigation, OPSEC, and the exploitation of oversharing.*

One relatively banal – yet important – association many advertisements make is between their services and the ability to navigate the Dark Web. This ability to navigate is informed by what I call 'OPSEC politics,' a social structure beyond the gaze of the surveillance-plagued Clear Web, where the advertisements promise to keep their patrons safe from corporations or law enforcement. In turn, OPSEC politics provides a justification for the exploitation of others – specifically, the exploitation other people's personal information. The fruits of this exploitation make up the bulk of the advertised products.

In sum, the dark magic system promises control over one's environment by exploiting the 'Clear Web' magic system. These features almost tell us more about surveillance capitalism than they do about the Dark Web. So, for good measure, we can also consider how the dark magic system itself collapses under the weight of its own absurdities: like the magic system Williams critiqued, the many of the associations and promises of Dark Web advertising dissipate under the most cursory of examinations. In this sense, like William's magic system, Dark Web advertising shows us the limits of imagination about how an anonymizing system might actually serve social needs.

Navigating the dark

A major association made by the advertisements served on search engine sites is the ability to find new onions, to trace the Dark Web, and to recognize 'legit' sites from scam sites. This can be readily seen in the advertisements for directories – collections of links –

and the surprising number of search engines advertising their services, even on other search engine sites. In many ways, this is redolent of the early 2000s, when Google's search competed with Yahoo's directory as key entry points into the Clear Web. Likewise, would-be Dark Web users might turn to the search engines to find things, or to directories, which collect and categorize links. (In fact, they're likely doing both, as well are relying on resources on the Clear Web, such as Reddit).

Many of the link directories or search engines present themselves as revealing scams or providing vetted links. One advertisement that I've seen over the years is the Tor Scam List, which claims to name and shame Tor vendors and sites that are fraudulent. Conversely, advertisements for single vendors or multi-vendor markets associate themselves with trustworthiness, using 'trusted' or 'verified' in their advertisements, or put various logos of ostensibly legitimate authorities (Reddit, DeepDotWeb, or a search engine logo) on their sites to present themselves as legit.

The dark magic association here is clear: perhaps the Dark Web is a terrifying place for outsiders, but, armed with the advertised services and links, we can conquer the dark, easily tell friend from fraudster, and find the products we need.

OPSEC politics

Mere navigation is not enough, however. The dark magic system also promises operational security (OPSEC). Originally developed by the U.S. military during the Vietnam War (Redacted 1993), OPSEC has become a term of art, particularly among users of the Dark Web. Perhaps the clearest definition of OPSEC comes from security researcher The Grugq, who says that OPSEC simply means:

> keep your mouth shut. Don't say it. The less you say, the harder it is for people to figure out what you're doing . . . In short, shut the fuck up (The Grugq 2012).

Essentially, having good OPSEC means not revealing personal information – name, age, gender, location. The central values are secrecy and distrust. Encryption of connections and messages, mixing of currencies and network traffic are among the techniques of choice. This privacy mentality has become an underlying ethos for many on the Dark Web, becoming what I call OPSEC politics, 'a rational means to structure relationships and, from there, conceive of a social order' (Gehl 2018, 112).

Adhering to this disposition, the dark magic system promises to maintain anonymity, even as we buy from vendors. The Hidden Marketplace promises, 'You can be assured of your safety and anonymity. We mix your bitcoin and encrypt messages and personal information.' Another common advertiser, easyCards, uses what Rachel-Heath Ferguson (2017, 694) calls 'OpSec Linguistics':

> Why do you write messages using so weird language/making mistakes?
>
> That's important rule we also would recommend you to follow. First of all - we don't want to let anybody know our location. Speaking English using some words more frequently than the others may expose our native language. Thanks to writing in weird but understable style, we are sure about impossibility to track our roots using that way.

The occasional advertisements for Dark Web social media also adhere to OPSEC politics. A Dark Web social networking site advertises itself: 'tired of surveillance? Enjoy freedom of speech and privacy.' After joining the social network, a user can enjoy the same affordances of Facebook: sharing media, liking posts, and making (pseudonymous) friends, but with no oversight from a centralized corporation. In this case, one of the promises of the dark magic system is an escape from surveillance capitalism.

Exploitation of personal information

To those invested in Dark Web OPSEC politics, Clear Web practices are derided as 'oversharing.' Oversharing is seen as a loss of control, a naive and foolish giving away of personal information. In contrast, the hardcore OPSEC of the Dark Web is heralded as a rational response to the surveillance society. As one Dark Web search engine site (which sells advertising space) puts it, 'In a world where everyone is over exposed, the coolest thing you can do is maintain your mystery!' And the dark magic system promises the ability to exploit the information of those who overshare.

Take, for example, influencer cultures. These are micro-celebrities who build followings in corporate social media, particularly Instagram (Abidin 2015). They share their lives and engage in interactions with their loyal followers. Influencers seek to develop relationships with audiences by being 'authentic,' performing a reality that is accessible and yet entertaining for their followers (Duffy and Hund 2019). Influencers win at the logics of corporate social media – they gain likes, followers, comments. They produce themselves through corporate social media, which means they produce a great deal of data about themselves. Not all social media users are influencers, of course, but the logic of influencing reflects the general logic of corporate social media: share. Be open. Connect with others.

What the dark magic system reveals is that those who adhere to the logics of corporate social media may see their openness exploited. The ill-gotten fruits of oversharing are offered for sale in the dark magic system. One market advertising itself offers hacked Facebook accounts. Another market features vendors selling 'fullz,' or 'complete identities, which include name, address, email address, phone number, date of birth and Social Security number' (O'Rourke 2016). Many vendors and markets offer carding services – that is, stolen gift cards or credit card information.

The advertisements for these stolen data promise access to corporate social media accounts or easy money based in part on information that others – predominantly social media users – have shared. As security researchers have shown, the data that inform credit card fraud and identity theft are often gathered via Clear Web social media. The information people share on social media allow illicit data brokers to 'to put the pieces of someone's identity together' and thus gain access to their financial accounts ('Criminals Target UK Youth as Identity Fraud Rises 2016). As cybersecurity researcher Jason Nurse argues, identity theft is often achieved through 'the monitoring of individuals on social media as they post and interact online' (Nurse 2019, 10). Nurse argues that data thieves exploit 'the nature to overshare [and] the poor management of security and privacy online' (Nurse 2019, 10).[2]

The exploitation of 'oversharing' is the same logic that drives so-called 'revenge pornography,' a form of 'non-consensual pornography, sexually explicit photographs that were exchanged in a trustful communicative space are made public or are shared without the permission of the depicted individual; with harmful consequences' (Venema and Lobinger 2017).[3] Some of the marketplaces advertising on Dark Web search engines include vendors selling 'Nude sex pictures from many ex girlfriends.' Such sites have appeared on the Dark Web for years. In these instances, those who upload, sell, or consume the images justify doing so by arguing that the 'girlfriends' should not have shared their nude photos online, implicitly faulting the women for having bad OPSEC. Like any justification of the exploitation of personal information, this is another instance of victim blaming.

Don't believe in dark magic

Can we use this dark magic? Can we buy something more than counterfeit money, hacking services, or gold bullion? Will the dark magic incantation – navigation, OPSEC, and the ability to exploit the Clear Web users – lead to Dark Web success? Can we reliably exploit the fruits of surveillance capitalism while still escaping its ever-watchful eye?

Perhaps. I cannot truly say – I have not used a methodology that can reveal any truths in Dark Web advertising. I haven't bought or sold any products or placed any advertisements on any search engines – nor do I see an Institutional Review Board allowing for such activities! But, given the sheer number of advertisements, vendors, and markets I've observed, I will say it's entirely possible that stolen personal information, credit card data, drugs, guns, and bitcoins are changing hands on the sites and services advertised on general-purpose, Dark Web search engines.

Even still, I don't recommend we believe in dark magic. A range of problems haunt the dark magic system. And the vast majority of them involve the desire to scam other Dark Web users, rather than offer legit services to them.

First, the most notorious problem of Tor onion services is 'cloning,' where 'legit' sites are duplicated by scam sites (Steinebach et al. 2019, 9). Given that Tor URLs are alphanumeric strings (for example, a1b2c3d4e5f6g7h8.onion, or even 52 alphanumeric characters) that are not easily memorized by humans, it's easy to establish a site with nearly the same information but at a different URL – a 'cloned' onion. What's the difference between a clone and an original? Beside the operator, the clone often uses a different Bitcoin address.

Cloning affected my collection of advertisements. While I was examining search engines and gathering banner advertisements for this study, I found multiple instances of the Torch search engine, a popular search service. I initially thought they were mirrors, or redundant servers. Closer examination revealed subtle differences that indicate that Torch is aggressively being cloned. I found over two dozen Torch URLs. I gathered the advertisements on six of them and started comparing the advertisements' URLs. I found that each of the Torch clones pointed to more clones, this time of the Tor Scam List, which offers 'verified sites'. Each of the Tor Scam List clones, in turn, pointed to more clones, this time of sites such as easyCards and the HD Wiki, with more URLs and, tellingly, different Bitcoin addresses (in case anyone wanted to donate money to support the site). And, in a dark magic circle of cloning, these clones pointed to more clones of Torch. Clearly, someone is trying to intercept bitcoins, advertisement revenues, logins, or network traffic – likely for defrauding Dark Web consumers.

Similarly, another problem is the fact that there is no intellectual property protections on the Dark Web. An egregious example is a site claiming to be a 'Partner Company' of the search engine DuckDuckGo. This site offers a search bar labelled as 'DuckDuckGo' but is selling banner advertisements around that search box. It even has a DuckDuckGo favicon. But it's clearly not DuckDuckGo; it's just an attempt to capture some of that popular site's traffic. Moreover, this site's sole purpose seems to be to direct users to a 'Lucifer Market' – many of the advertisements it runs are for this market (though they appear to be for other things, including hitmen for hire).

And none of this is to speak of the fact that buying on the Dark Web is riddled with fraud, ranging from products not being delivered to large-scale exit scams perpetrated by market operators.

These problems are faced by would-be buyers perusing the dark magic system. But perhaps the biggest flaw in the dark magic system is the burden that would-be *advertisers* face. Cloning, phishing, and other deceptions indicate that the search engine sites one might want to place an advertisement on may not be the actual search engine site one is trying to advertise on. Thus, even buying advertisements in the dark magic system is problematic: how do you know that the advertisement space vendor you're working with is legit? How do you know you're exchanging bitcoins for advertising space? On TorDex, a search engine, the operator put up a warning: 'tordex@elude.in is the only email, do not send payments to anyone else for advertisements!' That sounds legit. Unless it's not.

And even if we manage to advertise on a 'legit' site, how do we know how our advertisement is performing? Recall that Tor is an anonymizing network. The standard advertising metrics, such as counting clicks, unique visitors, or impressions, are deeply problematic because Tor onions do not log traffic like standard websites. Thus, any claims based on unique visitors can be gamed. And yet, the sites selling advertising space brag about their metrics. As one Dark Web search engine boasts, 'Advertise with us! … Our search engine recives [sic] millions of unique views a month and your advertisement will be shown to real users of the dark net looking to buy.' A Dark Web advertisement network says 'transparency matters' and boasts that it has served over 9 million 'total unique impressions.' Perhaps the best clue as to how well these numbers can be gamed comes from Daniel's Hosting, a respected hosting service on Tor. Daniel's Hosting includes code to embed an old-school, 1990s-style hitcounter on your onion site. But, in a tip of the hat to the unreliability of these statistics, his hitcounter allows you to 'preload' it with as many hits as you like, which he notes is useful for, as Daniel's admits, 'faking' your numbers.

Again, to be fair, there's clearly commerce happening on the Dark Web, and moreover, enterprising entities are trying to clean up the Dark Web magic system with advertisement brokerage networks, brokering deals between advertisers and search engines, among other sites. But even this approach is subject to the same uncertainties – cloning, obscure URLs, and bogus metrification.

Ultimately, the dark magic system – particularly advertisements appearing around the general-purpose search engines that I have discussed in this paper – collapses under the weight of its own absurdities. This might be best illustrated by who's *not* advertising. When it comes to the dark magic system, it is rare for a reputable market – the kind of market subject to serious research (e.g. Espinosa 2019; Pace 2017; Bancroft and Peter 2016; Barratt and Maddox 2016) – to advertise their presence via the general purpose search engine banner advertisements I've encountered. As of this writing, legit markets – which is to say, markets where one can more reliably buy the product one is trying to buy – tend not to advertise on these search engines. One exception may be for the White House Market, but there was only one advertisement for White House in my collection, and I have rarely seen other 'legit' markets advertise in this manner.[4]

The dark magic system falls apart under the most cursory of examinations. The sheer number of clearly scam sites (Bitcoin doublers being the most common example), the anxious uncertainty that the advertisement even links to a legit site, the laughable gestures towards Clear Web metrics like 'impressions,' and the high likelihood that the sites advertised are short-term grifts, all demonstrate the illusory nature of this system.

Conclusion

All of the factors that reveal dark magic advertising for the illusion that it is beg the question: what is the Dark Web for? Is it an unethical reflection of the Clear Web? Is it a haven for exploitation, cruelty, and con artistry? Is it the highest expression of libertarian economics?

Raymond Williams's core argument about the 'magic system' of advertising points to another answer. His central criticism is not that advertising is crude, but that 'advertising is the consequence of a social failure to find means of public information and decision over a wide range of everyday economic life' (Williams 2000). For Williams, advertising is a symptom of the failure of capitalism to fulfill human needs. When a product or practice is associated with something more – something that we cannot clearly say the product provides – 'we have a cultural pattern in which the objects are not enough but must be validated, if only in fantasy, by association with social and personal meanings which in a different cultural pattern might be more directly available' (Williams 2000). Being anonymous and connecting with one another, the dark magic system tells us, is not enough: one must have more, one must become a master of OPSEC and an exploiter of anyone who is not as skilled in staying anonymous.

This is made all the more tragic when we consider how the Dark Web's magic is built in part on the exploitation of Clear Web surveillance. Trevor Smith sums up the contradiction quite well:

> From Edward Snowden's revelations about extensive government spying, we know that there is a possibility that all of our online actions, no matter how private we hope them to be, are being watched. At the same time, we are constantly warned of the dangers of online anonymity which can facilitate everything from illegal criminal activity to abusive trolling. Both of these contradictory aspects of the how online space operate point to it being characteristic of the social realm (Smith 2017, 36).

In the dark magic system, the most common social relations imagined for the anonymizing Dark Web are those of exploitative commerce – at best, scams, and at worst, the illegitimate exploitation of how we're legitimately exploited in corporate social media. This is in stark contrast to many of the creative aspects of anonymity (Beyer 2014, 6–7), as well as the long tradition of anonymity in service to political debate.

As Smith argues:

> Political speech and action are risky and require courage. The shield of anonymity has been, and continues to be, essential to the expression of dissenting points of view. If politics is to maintain its agonistic edge and not devolve into anti-political consensus, then making it easier to take part by shielding one's private life from one's public statements is necessary (Smith 2017, 111).

The Dark Web can indeed make it easier for such a shield to exist. The problem is that this affordance is largely ignored in the dark magic system of search engine advertising in favour of a rapacious individualism. Like the magic system in general, the dark magic system purports to be a way to fulfill social relations through consumerism, but it can never do so. The deeper social needs we have – solidarity, the end of exploitation, including the end of our being exploited by corporate social media – will never be filled by magic, dark or otherwise. Rather than presenting the Dark Web as an antidote to the rampant consumerism of the Clear Web, an alternative to surveillance capitalism where social relations beyond the gaze can bloom, the dark magic system presents itself solely as a dark and cloudy mirror to surveillance capitalism.

Notes

1. Unless either party reveals their identity. For an example, see Facebook's onion service, facebookcorewwwi.onion.
2. In addition to gathering information via social media, carders and fullz vendors also glean information from data breaches. While this is not necessarily tied to what the OPSEC-minded might call 'oversharing,' a data breach is also indicative of the excesses of personal information gathering happening in surveillence capitalism.
3. As I discuss in *Weaving the Dark Web*, I would avoid labelling the non-consensual sharing of someone's images as 'pornography.' I draw on Barbara DeGenevieve's definition of pornography as 'consensual acts being depicted … for the sexual arousal and masturbatory entertainment of the viewer.' Thus, for DeGenevieve, rape scenes, snuff, abuse, and child sex images are not pornography: they are non-consensual, and thus 'prosecutable crimes' (DeGenevieve 2007, 235). By that definition, so-called 'revenge porn' images are evidence of a crime, not pornography.
4. The only locations serving banner advertisements that likely lead to the market or product advertised are specialized sites like Recon, a site that is attempting to inherit the legitimacy of Grams. Recon is a specialized search engine, focusing predominantly on drug vendors, rather than a general-purpose search engine promising an index of all Tor onion sites.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Notes on contributor

Robert W. Gehl is the F. Jay Taylor Endowed Research Chair of Communication at Louisiana Tech. His books include*Reverse Engineering Social Media* (Temple 2014), *Weaving the Dark Web* (MIT 2018), and *Social Engineering* (MIT 2022).

References

Abidin, C. 2015. “Communicative ❤ Intimacies: Influencers and Perceived Interconnectedness.” *Ada New Media* (blog). 1 November 2015. https://adanewmedia.org/2015/11/issue8-abidin/

Bancroft, A., and S. R. Peter. 2016. “Concepts of Illicit Drug Quality among Darknet Market Users: Purity, Embodied Experience, Craft and Chemical Knowledge.” *International Journal of Drug Policy* 35 (September): 42–49. doi:10.1016/j.drugpo.2015.11.008.

Barratt, M. J., and A. Maddox. 2016. “Active Engagement with Stigmatised Communities through Digital Ethnography.” *Qualitative Research* 16 (6) (May): 701–719. doi:10.1177/1468794116648766.

Beyer, Jessica L. 2014. *Expect Us: Online Communities and Political Mobilization*. Oxford; New York: Oxford University Press.

‘Criminals Target UK Youth as Identity Fraud Rises.’ 2016. “CIFAS.” 5 July 2016. https://www.cifas.org.uk/newsroom/criminals-target-uk-youth-as-identity-fraud-rises

DeGenevieve, B. 2007. “Ssspread.Com: The Hot Bods of Queer Porn.’.” In *C’lickme: A Netporn Studies Reader*, edited by Katrien Jacobs, Marije Janssen, and Matteo Pasquinelli, 233–236. Amsterdam: Institute of Network Cultures.

Duffy, B, and E. Hund. 2019. “Gendered Visibility on Social Media: Navigating Instagram’s Authenticity Bind.” *International Journal of Communication* 13: 20.

Espinosa, R. 2019. “Scamming and the Reputation of Drug Dealers on Darknet Markets.” *International Journal of Industrial Organization* 67 (December): 102523. doi:10.1016/j.ijindorg.2019.102523.

Ferguson, R. 2017. “Offline ‘Stranger’ and Online Lurker: Methods for an Ethnography of Illicit Transactions on the Darknet.” *Qualitative Research* 17 (6): 683–698. doi:10.1177/1468794117718894.

Fuchs, C. 2012. “The Political Economy of Privacy on Facebook.” *Television & New Media* 13 (2): 139–159. doi:10.1177/1527476411415699.

Gehl, R.W. 2016. “The Politics of Punctualization and Depunctualization in the Digital Advertising Alliance.” *The Communication Review* 19 (1): 35–54. doi:10.1080/10714421.2016.1128187.

Gehl, R.W. 2018. *Weaving the Dark Web: Legitimacy on Freenet, Tor, and I2P*. Cambridge, MA: MIT Press.

The Grugq. 2012. “OPSEC: Because Jail Is for Wuftpd.” 21 May 2012. https://www.youtube.com/watch?v=9XaYdCdwiWU

Nurse, J. R. C. 2019. “Cybercrime and You: How Criminals Attack and the Human Factors that They Seek to Exploit.” *ArXiv:1811.06624 [Cs]*, May. 662–690. doi:10.1093/oxfordhb/9780198812746.013.35.

O’Rourke, M. 2016. “The Costs of Low-Tech Hacking.” *Risk Management* 63 (7): 40.

Pace, J. 2017. “Exchange Relations on the Dark Web.” *Critical Studies in Media Communication* 34 (1): 1–13. doi:10.1080/15295036.2016.1243249.

Redacted. 1993. “Purple Dragon: The Origin and Development of the United States Opsec Program.” Series VI, Vol. 2, No. 609. United States Crytologic History. Fort Meade, MD: National Security Agency. Accessed 2017-02-09. https://www.nsa.gov/news-features/declassified-documents/cryptologic-histories/assets/files/purple_dragon.pdf

Smith, T.G. 2017. *Politicizing Digital Space*. University of Westminster Press: London. Accessed 2017-06-26. https://doi.org/10.16997/book5

Stark, Luke. 2018. “Algorithmic Psychometrics and the Scalable Subject.” *Social Studies of Science* 48 (2): 204–231. doi:10.1177/0306312718772094.

Steinebach, M., M. Schäfer, A. Karakuz, K. Brandl, and Y. Yannikos. 2019. “Detection and Analysis of Tor Onion Services.” In *Proceedings of the 14th International Conference on Availability, Reliability and Security*, 1–10. ARES ’19. New York, NY, USA: Association for Computing Machinery. 10.1145/3339252.3341486.

Venema, R., and K. Lobinger. 2017.“And Somehow It Ends up on the Internet.’ Agency, Trust and Risks in Photo-Sharing among Friends and Romantic Partners.” *First Monday*, July. doi:10.5210/fm.v22i7.7860.

Williams, R. 1960. “The Magic System.” *New Left Review*, June 1960. Accessed 2020-11-09. https://newleftreview.org/issues/I4/articles/raymond-williams-the-magic-system

Williams, R. 1993. “Advertising: The Magic System.” In *The Cultural Studies Reader*edited by Simon During, 410–423. London and New York: Routledge.

Williams, R. 2000. “Advertising: The Magic System.” *Advertising & Society Review* 1 (1). doi:10.1353/asr.2000.0016.