SAGE reference

# The SAGE Encyclopedia of the Internet

## Dark Web

Contributors: Monica J. Barratt, Judith Aldridge & Alexia Maddox
Edited by: Barney Warf
Book Title: The SAGE Encyclopedia of the Internet
Chapter Title: "Dark Web"
Pub. Date: 2018
Access Date: June 6, 2018
Publishing Company: SAGE Publications, Inc.
City: Thousand Oaks,
Print ISBN: 9781473926615
Online ISBN: 9781473960367
DOI: http://dx.doi.org/10.4135/9781473960367.n59
Print pages: 185-188

©2018 SAGE Publications, Inc.. All Rights Reserved.
This PDF has been generated from SAGE Knowledge. Please note that the pagination of the online version will vary from the pagination of the print book.

Copyright © 2018 by SAGE Publications, Ltd.

The dark web (also referred to as the darknet, the hidden web, or the hidden Internet) consists of websites that use anonymity tools, usually Tor or I2P, to hide the IP (Internet Protocol) addresses of their servers so that their physical location cannot be determined. This entry defines the dark web and discusses how it differs from the clear web, how it is used, myths about the dark web, and the future of the dark web.

Websites on the dark or hidden web can only be accessed via anonymity tools such as Tor and I2P and are also not available for standard search engines such as Google to index. Tor hidden services have URLs ending in .onion, referencing the routing technique that—with multiple layers of encryption resembling an onion—enables anonymous communication over computer networks. The dark web grew in size and cultural significance in the 2010s, especially following the launch of the first anonymous online market reliant on Tor and Bitcoin, Silk Road, in 2011.

## Dark Web Versus Clear Web

The dark web utilizes the public Internet, which originated as a decentralized communications channel developed through the U.S. military (ARPANET, first proposed in 1967). Its user interface (the World Wide Web) was invented in 1989 as a decentralized knowledge sharing and user-produced environment developed by a researcher at CERN, Tim Berners-Lee. The public access Internet gained social uptake in the 1990s, creating trade-offs over time for the user between regulation and surveillance versus freedom and anonymity.

The tension between regulation and freedom has resulted in at least two ways of accessing and engaging with content online: (1) the clear web and (2) the dark web. The clear web, also known as the surface web, is a user-friendly environment, much of which is composed of user-produced content in commercially curated environments. Content on the surface web can be indexed by search engines such as Google. In contrast, the dark web is an encrypted environment offering greater privacy with the price of a less user-friendly experience.

In the clear web, user requests (connections) are relayed directly to the Internet service provider (ISP) and from there to the desired destination using the shortest possible path. However, this unencrypted connection enables network surveillance or traffic analysis, which has facilitated business models that develop content, software, and platforms to provide free services that people will use in exchange for access to identifying information.

Due to the unencrypted nature of the clear web, the digital traces of identifiable user activities such as browsing behaviours can be collected. Users are also requested to give personal information when they sign up for a service. Information provided by users and gleaned from their online behaviour may then be used by a company to target advertising or for research purposes, as when Facebook manipulated users' newsfeeds to show them either more positive or more negative emotional content as part of a study on emotional contagion. This information may also be sold for advertising and marketing purposes or provided to law enforcement to enhance surveillance or prosecution. Consequently, use of the clear web environment involves a trade-off for users where the use of free services results in the loss of privacy and individual lack of control over how personal information is used.

Surveillance is conducted using data generated by citizens who use the clear web. Governments use these data to understand their citizens, police to identify illegal activities, public health professionals to predict the next disease outbreak, and commercial enterprises

Copyright © 2018 by SAGE Publications, Ltd.

to better understand consumers and develop new markets. Through the revelations of former U.S. National Security Agency contractor Edward Snowden, the public has become more aware of the trade-off between usability and surveillance that their use of the clear web now entails. There is a growing understanding that activities in the clear web may result in the loss of personal privacy, may have long-term social and professional repercussions, and may bring unwanted attention by regulatory bodies and by individuals who may have malicious intent, including scammers, hackers, and trolls.

Tor as an anonymity tool offers a potential solution to the modern dilemma of pervasive digital surveillance. Onion routing was developed by the U.S. Naval Research Laboratory in the mid-1990s to protect government and especially intelligence communication from surveillance. The Tor program, based on onion routing, was launched in 2002. Tor was originally an acronym for The Onion Router, but is now used as a word of its own: Tor means “gate” or “door” in German.

Tor enables private communication and anonymous online browsing and circumvents location-based censorship of webpages through anonymizing user IP addresses. To achieve this, the Tor browser directs Internet traffic through a volunteer network, consisting of more than 7,000 relays at the time of publishing, to conceal a user’s exact location and prevent attackers from linking communication partners. So it is apt to observe that the dark web, accessed primarily through Tor, is an anonymized and therefore “hidden” location for Internet users.

The dark web and clear web environments are interconnected. Tor can be used to browse any website in the clear web, and there are many bridging websites linking clear and dark web content. Although Tor can be used to access the clear web, doing so results in a less efficient user experience due to reduced usability of the interface, the lack of searchability of information held on the onion router, and the reduced speed of loading.

In many ways, the dark web usage experience is similar to the earlier years of web browsing in the 1990s before the Google era. To find content in the dark web, a user usually needs to know the direct URL for the desired website. However, several indexes are available both on the clear and dark web to direct the would-be dark web user, and some dark web search engines are now available, including Grams, which indexes listings from darknet markets.

## Uses of the Dark Web

Although the dark web as understood here has existed since the mid-1990s, this hidden encrypted location for Internet activities was first brought to the world’s attention by Silk Road, a marketplace for illegal drugs, in 2011. Darknet drug markets such as Silk Road and its many successors function like eBay- or Amazon-style marketplaces in that they host multiple sellers and aggregate and display customer feedback ratings and comments. These marketplaces, known as cryptomarkets, function as a third party or broker by holding payments until customers receive and are satisfied with their shipments, and by adjudicating in the event of dispute. Participants transact anonymously not just via their darknet location but also through the use of cryptocurrencies such as Bitcoin for payment. Policy and legal responses to the dark web have been in part shaped by the rise of cryptomarkets and their facilitation of the global illegal drug trade.

However, the drug trade is only one of a number of activities that occur within the dark web, which may best be understood by the types of content available rather than the distinct nature of its services. The types of content available in the dark web may be categorized into

Copyright © 2018 by SAGE Publications, Ltd.

five types. The first type is largely for entertainment value and can include content that is heavily regulated in the clear web such as pornography. Another style of content is self-referential material for how to use Tor, how to set up hidden services, or how to use encryption to enact technical anonymity, alongside guidelines for conventions and practices for social anonymity.

As described earlier, the third type of content includes marketplaces and commercial ventures that specialize in illicit or heavily regulated commodities, such as cryptomarkets that facilitate the sale of drugs, guns, and other digital commodities such as stolen credit card information and fake identity documents. A fourth area of content that is not mutually exclusive to the other areas is related to scam and phishing sites, hoaxes, and fraud services.

The fifth category of dark web content includes services in which users themselves determine the purposes and contents of communication or uses of Tor, such as anonymous email programs, chat services, social networks, open topic forums, and peer-to-peer file sharing. While this content can mirror the content described earlier, it also offers a space that is free of the threat of surveillance, political interference, and censorship. Activist groups can utilize the dark web to publish or share content that would otherwise be dangerous for them to publish through the clear web. The use of anonymizing software such as Tor to anonymously access clear websites that are banned or firewalled in certain countries also facilitates information access and freedom of speech.

## Dark Web Myths

When the dark web has entered the public imagination, it is often through the filters of mainstream media channels, which have largely represented the dark web as a large and shadowy haven of illegal activity. Chief among the myths that have arisen about the dark web is that it is several times larger than the clear web. The evolution of this myth relates to the confusion between the terms *dark web* and *deep web*.

The deep web primarily refers to Internet content that cannot be indexed by search engines, but it does not necessarily require anonymizing software to access. This content may be locked behind paywalled websites or company or academic databases, and it includes websites that are not linked to other websites, private websites and forums, and large amounts of social networking site content, such as private Facebook group content.

Dark web content may be understood as a very small subset of deep web content, differentiated by being intentionally hidden and requiring anonymizing software to access. While there are estimated to be billions of sites in the clear or surface web, the number of dark web sites is estimated at less than 30,000, leading *Wired* to describe the dark web as “more like a dark nook” (Cox, 2015, n.p.).

The *Wired* article, by Joseph Cox, also notes that the association between the dark web and nefarious activity ignores that most types of content available on the dark web are also available on the clear web. For example, although the dark web is infamous for its facilitation of communities of child pornography traders, the Internet Watch Foundation found more than 30,000 URLs containing child porn images that included only 51 hosted on the dark web. The belief that the dark web is impenetrable by law enforcement has also been discredited by the growing number of arrests of participants and leaders of drug cryptomarkets and dark web paedophile rings. Traditional policing techniques, including undercover operations, can also succeed in digital environments.

Copyright © 2018 by SAGE Publications, Ltd.

## Future of the Dark Web

Wide-reaching digital surveillance has become embedded in the lives of most of the world's citizens, with many governments pushing for expanded access to these vast amounts of personal digital data. As the consequences of pervasive digital surveillance become increasingly apparent, more people may choose to utilize Tor and the dark web to exercise freedom of speech and access the kind of privacy that generations before took for granted. Although it is clear that many types of crime thrive in the anonymous environment made possible by Tor and the dark web, its value as a platform for communication without undue state interference may increase in such future worlds of high surveillance and eroded privacy.

***See also*** Bitcoin; Child Pornography and the Internet; Cybercrime; Cryptocurrencies; eBay; Internet Censorship; Internet Surveillance; Peer-to-Peer Networks

## Websites

Tor Project: https://torproject.org/

Monica J. Barratt Judith Aldridge Alexia Maddox
http://dx.doi.org/10.4135/9781473960367.n59
10.4135/9781473960367.n59

**Further Readings**

Barratt, M., & Aldridge, J. (2016). Everything you always wanted to know about drug cryptomarkets* (*but were afraid to ask). International Journal of Drug Policy, 35, 1–6.
Bartlett, J. (2014). The dark net. London, UK: Random House.
Cox, J. (2015, June 18). The dark web as you know it is a myth. Wired. Retrieved from https://www.wired.com/2015/06/dark-web-know-myth/
Gehl, R. W. (2016). Power/freedom on the dark web: A digital ethnography of the dark web social network. New Media and Society, 18, 1219–1235.
Quintin, C. (2014, July 1). 7 Things you should know about Tor. Electronic Frontier Foundation. Retrieved from https://www.eff.org/deeplinks/2014/07/7-things-you-should-know-about-tor