What is the dark web and how does it work?

October 20 2016, by Daniel Prince

Credit: AI-generated image (disclaimer)

We often hear about the dark web being linked to terrorist plots, drug deals, knife sales and child pornography, but beyond this it can be hard to fully understand how the dark web works and what it looks like.

So just for a minute imagine that the whole internet is a forest – a vast expanse of luscious green as far as the eye can see. And in the forest are well worn paths – to get from A to B. Think of these paths as popular

search engines – like Google – allowing you as the user the option to essentially see the wood from the trees and be connected. But away from these paths – and away from Google – the trees of the forest mask your vision.

Off the paths it is almost impossible to find anything – unless you know what you're looking for – so it feels a bit like a treasure hunt. Because really the only way to find anything in this vast forest is to be told where to look. This is how the dark web works – and it is essentially the name given to all the hidden places on the internet.

Just like the forest, the dark web hides things well – it hides actions and it hides identities. The dark web also prevents people from knowing who you are, what you are doing and where you are doing it. It is not surprising, then, that the dark web is often used for illegal activity and that it is hard to police.

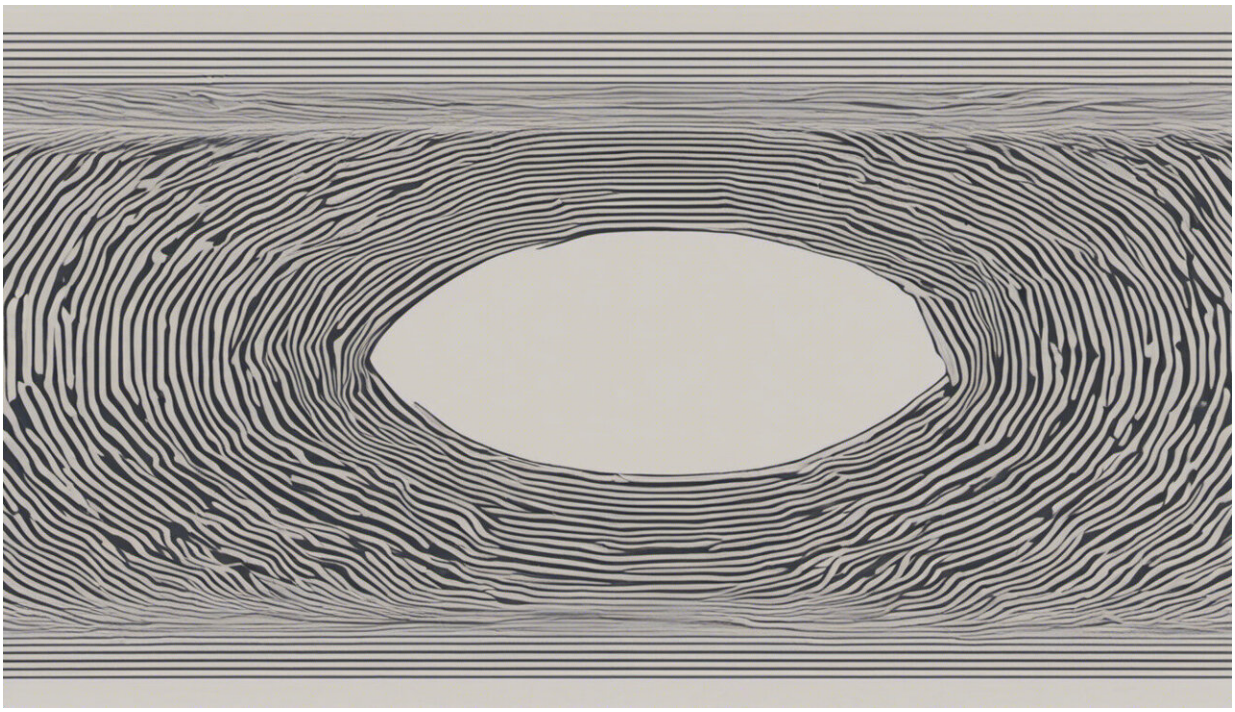
Technical challenges

Dark web technologies are robustly built without central points of weakness, making it hard for authorities to infiltrate. Another issue for law enforcement is that – like most things – the dark web and its technologies can also be used for both good and evil.

So in the same way criminals use it to hide what they are up to, it can also help groups fight oppression or individuals to whistle blow and exchange information completely anonymously. In fact, Tor – "free software and an open network that helps you defend against traffic analysis" and a critical part of the so-called dark web – has been funded by a range of Western governments, including the US.

A service like Tor, is global, in no one physical location, and is operated by no one commercial entity – which is typical of these technologies.

Theoretically, the only way to intercept communications sent via something like Tor is to install a "backdoor" in the application everyone uses. A backdoor is meant to provide a secret way to bypass an application's protection systems – in a similar way to how people hide backdoor keys in flower pots in the garden in case they get locked out of their house.



Credit: AI-generated image (disclaimer)

However, the use of a "backdoor" could also allow any governments – even oppressive ones – to intercept communications. Indeed, cyber breaches have shown us that any backdoor or weakness can be found and exploited by hackers in order to steel people's information, pictures and data.

Exploiting the darkness

Of course, none of this is new – criminals have always found ways to communicate with each other "under the radar". Mobile phones have been used by criminal gangs to organise themselves for a long time, and as a society we are comfortable with laws enabling police to tap telephones and catch criminals.

Unfortunately, infiltrating the dark web is not quite as easy as tapping the local telephone exchange or phone network. Because the dark web is quite unlike the telephone system – which has fixed exchanges and is operated by a small set of companies, making interception easier.

Even if tapping the dark web was a straightforward exercise, morally it is still fraught with questions. In the UK, the Draft Investigatory Powers Bill, dubbed the snoopers' charter, sets out the powers and governance for Law Enforcement over communications systems. However, the discussion of the bill has been impacted by the Snowden revelations which have demonstrated that society is not comfortable with mass, unwarranted surveillance.

Surveillance society

This public distrust has led to many technology companies pushing back when it comes to accessing users' devices. We have seen Microsoft take on the US government over access to email and Apple against the FBI when petitioned to unlock an iPhone of a known terrorist.

And yet some of these same communications companies have been harvesting user data for their own internal processes. Famously, Facebook enabled encryption on WhatsApp, protecting the communications from prying eyes, but could still look at data in the app

itself.

For now, though, it is clear that we still have a long way to go until society, government, law enforcement and the courts settle on what is appropriate use of surveillance both on and offline. And until then we will have to live with the fact that the one person's freedom fighting dark web is another's criminal paradise.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation