Chapter 101
Privacy, Ethics, and the Dark Web

Richard T. Herschel
Saint Joseph's University, USA

ABSTRACT

This article examines the impact that dark web activities are having on society. Hacking and data breach activities have created serious challenges to cybersecurity leading to new data privacy legislation in Europe and the United States. The dark web is a segment of the web where people employ special browsers that can mask their identity and hide their network activity. Here can be found a wide range of illicit activities that are oftentimes criminal in nature, including sales of stolen documents, the information of others, and other contraband. Companies are actively trying to monitor dark web activities because new legislation requires them to inform authorities if a breach compromising data privacy has occurred; otherwise, they can be penalized. It is argued that as governments act to reign in dark web activities, they must employ an ethical perspective that is grounded in theory to weigh the intentions of darknet actors and their impact. This is due to the fact that some dark web activities such as whistleblowing can actually benefit society.

INTRODUCTION

Online activities that have compromised people's privacy has led to the creation of legislation that is intended to protect privacy rights. These decrees represent an attempt by law enforcement and government officials to more forcefully address immoral patterns of online behavior that are effectively compromising the safety of society. Two primary examples of this new legislation are the European Union's General Data Protection Regulation [GDPR] and the California Consumer Privacy Act. Both detail rules and procedures that organizations must follow when handling the personal information that they collect online as well as the rights afforded to the individual in the management of their digital identity.

The GDPR states that EU citizens have the right to information about them that is being collected by organizations as well as how it is being processed. They can ask that incorrect, inaccurate, or incomplete personal data be corrected or that their personal data be erased. Individuals can restrict the processing of

DOI: 10.4018/978-1-7998-8954-0.ch101

their personal data for marketing purposes or for any other given situation they deem necessary. People can even request that decisions based on automated processing concerning them be made by people, not only by computers (EU Commission (1), 2018). The GDPR defines personal data to include any information generated by organizations that monitors citizen behavior and generates personal information. This includes all forms of tracking and profiling on the internet, including for the purposes of behavioral advertising.

California has passed new consumer-privacy legislation that is somewhat similar to the GDPR - California Consumer Privacy Act, A.B. 375. This law is the first of its kind in the United States. The California regulation requires businesses to offer consumers options to opt out of the sharing of their personal information, and it gives Californians the right to prohibit the sale of their personal data. The law also forbids retailers from treating customers who opt out of data sharing any differently from those who don't, suggesting the possibility that this provision could end loyalty programs that offer discounts to members. The regulation broadens the definition of what constitutes personal information and it gives enforcement power to the California attorney general (Vartabedian, Wells, and O'Reilly (2018).

While these legislative actions are intended to constrain organizations in their use of personal information collected online, there remains a high probability that continuing attempts will be made to compromise data privacy. Specifically, the illicit activities of entities employing the Dark Web present an ongoing and much more serious challenge to the protection of privacy rights than do the activities of legitimate organizations engaged in online business transactions.

Primarily off the mainstream radar until recently, the Dark Web is viewed by many as a haven for those who engage in unscrupulous behavior. Yet, at the same time it can also provide an important safe harbor for those engaging in whistleblowing activity. This paper examines the challenges that the Dark Web presents for society, its impact on privacy rights, and the ethical challenges that require organizations to be vigilant in order to minimize threats to both their clientele and to their operations. The paper also examines the important role that ethical theories play in shaping our views about Dark Web activities.

BACKGROUND

Hartnett (2017) states that when someone refers to doing online research on a topic or they are looking for other online information, they typically use search engines such as Google, Yahoo, Safari, and Bing. These applications employ information on the public [or surface] web, which represents only 4% of web content (~8 billion pages). The Deep Web refers to the other 96% of the digital universe that is basically hidden. Wolford (2018) notes that this is the bulk of the Internet and it differs from the surface internet that most people know and use, because it is not indexed by search engines. He reports that the Deep Web includes content such as financial databases, web archives, and secured documents.

Hewilson (2018) provides some interesting statistics about the Deep Web. The author reports that:

- the Deep Web contains 7500 terabytes of information where the surface web, in comparison, contains 19 terabytes of content,
- the Deep Web has between 400 and 550 times more public information than the surface web,
- more than 200,000 Deep Web sites currently exist,
- together, the 60 largest Deep Web sites contain around 750 terabytes of data, surpassing the size of the entire surface web 40 times,