Cybersecurity Legislation

Christopher Thomas Anglim
University of the District of Columbia, USA

INTRODUCTION

Nations throughout the world use cyberspace legislation to protect their cybersecurity and control criminal activity on the Dark Web. The Dark Web consists of underground websites and databases that are accessible anonymously using "The Onion Router" (TOR). Development of the technology operating TOR has frequently been attributed to the US Naval Research Laboratory. TOR protects the user's identity by routing ordinary location services and Internet Protocols (IPs) through several different nations. TOR is an example of a darknet, which is a closed, private network that operates on the more conventional Internet Protocols. Darknets bypass the TCP/IP to ensure anonymous, essentially untraceable global networks.

The US government had intended to use TOR to provide the means for activists in nations with repressive governments to communicate with each other, without their government becoming aware of their activities. TOR has, however, become a form of contemporary technology that provides criminals with swift and often anonymous means to move funds and goods to enrich themselves through a wide variety of illegal activities such as hosting malware, selling illicit drugs, disseminating child pornography, arranging for contract killings, conducting terrorist acts, and laundering money.

This chapter explains the role of the legislature on all levels in controlling criminal behavior on the Dark Web, including the purpose of cybersecurity legislation, different approaches legislation, and the benefits and limitations of the legislative approach. In the United States, Congress continues to consider federal legislation intended to control the widespread criminal behavior that occurs on the Dark Web, such as the sale and distribution of drugs, illegal weapons, and child pornography. This chapter begins with an introduction that explains the purpose behind legislation. This followed by the Background section, which provides an overview on the topic of Legislation and the Dark Web, the purpose of such Legislation. Because this topic involves the balancing of basic rights and duties, the section also discusses the constitutional issues involved. Much of the chapter deals with Congressional action to date on the Dark Web and what Congress still needs to do on this topic. The Chapter then discusses legislative action taken on the state level, the international level, and legislative action that other nations have taken. The chapter concludes with recommendations for creating a legislative regime that seeks to both control criminal behavior on the Dark Web and ensure that the Dark Web is available for those who use need it for legitimate purposes.

Understanding Legislation as Lawmaking

Legislation is law as enacted by a legislative body after it has considered a specific measure. Laws enacted by Congress, a parliament, a state legislature, or a city council are examples of legislation. In the American system, legislation usually becomes law after being approved by an executive (such as the President, Governor, or Mayor) or if the legislature overrides the executive's veto.

DOI: 10.4018/978-1-5225-9715-5.ch027

Legislation reflects policy considerations, meaning that it is subject to political concerns and preferences. The executive branch implements legislation and the judiciary reviews legislation. All laws require balancing between the individual's right to privacy and protecting the public's right to be protected. Liberty rights, including privacy rights are not absolute. These rights are balanced by the rights of other individuals and society. For nearly 30 years, legislatures on the local, state, and federal government have sought to prohibit certain types of behavior using computers as "cyber-crimes". This means that a government will prosecute individuals for violating the law and has imposed specific sanctions (such as fines and prison terms) for these violators.

As a very new type of law, cyberspace law remains a work in progress. While the principles of cybersecurity law are derived from the law governing other legal areas, not all of these precedents are designed to fit the current reality of cybersecurity. The Dark Web, especially, poses a large number of legislative challenges. These involve difficult issues of balancing the protection of free speech rights of individuals versus the need to protect the community from the online trade in a whole variety of illegal goods and services. Some of the many challenges in drafting cybersecurity law include that criminals freely use technology to maintain anonymity on the Web. This allows them to evade law enforcement with relative ease. The need for legislative action in controlling criminal activity on the Dark Web became particularly apparent as law enforcement agencies uncovered such sites as the "Silk Road", which were anonymous online markets for illicit and illegal goods. These online black markets allowed buyers to purchase illegal drugs and the transactions in bitcoin and conduct transactions anonymously, using "dummy" transactions to conceal the connection between buyers and sellers. By so doing, the Silk Road evaded The US's most advanced electronic surveillance technology. The site operated from 2011 until the Federal Bureau of Investigations (FBI) curtailed its operations in 2013. While in operation, the Silk Road amassed an estimated $1.2 billion in revenue. Other illicit sites such "Pandora Market" and "Hydra Marketplace" followed the Silk Road Model.

The situation has worsened grew worse over time. At the time law enforcement authorities force the site, Alpha Bay to close in 2017, that site had 200,000 users, 40 vendors, and was ten times the size of Silk Road. Alpha Bay indicated that buyers and sellers were scaling up their operations on the Dark Web.

At the same time, hackers operating in the Dark Web stole a large amount of private customer data from Equifax, a major consumer credit reporting agency. The hackers then demanded 600 Bitcoins (about $2.5 million) in exchange for the sensitive financial information of the 143 million people. The way that these criminals were able set up such a secret, untraceable criminal enterprise at such a massive scale led policymakers to doubt whether law enforcement had sufficient authority and technology to contend with the illicit Dark Web activities (Ghappour, 2017).

The Dark Web has also become a major marketplace of counterfeit and stolen medicine. Criminals have found that the return on investment of such products has been very high. This trade in harmful, useless, or expired medicines has tragically led to the deaths of many who relied on them.

BACKGROUND

Overview

Cyberspace is a virtual computer world. More specifically, is an electronic medium used to form a global computer network to facilitate online communication. This chapter focuses on recent cybersecurity legislation, seeks to determine the effectiveness of specific cybersecurity legislation, and present