

Censorship of Digital Resources Worldwide

Kari D. Weaver

University of South Carolina Aiken, USA

INTRODUCTION

Censorship is an issue that has impacted information access for as long as humans have shared information. As communication technologies have grown and changed, from oral traditions, to the printing press, to the rapid rise of the Internet, many have sought to limit the ability of others to create, find, use, and share information with their fellow citizens. This has had important implications for the power and freedom of individuals within these societies, and has helped to shape the face of the modern world.

Censorship is of critical importance for managers and entrepreneurs worldwide. Although international business has become increasingly “flattened” by globalization, information policy varies widely and has a significant impact upon both business climate and personnel safety. Employees in some countries may not be able to receive or share certain information, and government censorship may require additional functionality to be included in products or services. Cultural norms, practices, and ethical guidelines for capturing and sharing information are governed by the laws of the host nation. All of these factors must be accounted for when considering expanding operation into new locations around the globe.

BACKGROUND

Although censorship is a familiar concept, a precise definition is challenging. In this article, “censorship” is defined as “the action or the use of authority to limit access to information that would otherwise be available in the public sphere.” Common justifications for censorship include morality, obscenity, blasphemy, or national security. It can be performed by individuals, groups, corporations, or governments and their agents.

Censorship has existed throughout civilized history. The word “censor” is derived from Latin, when cen-

sors within the Roman Empire conducted the census and other state functions while regulating morality under Roman rule (Pina Polo, 2012). Censorship has been practiced worldwide, primarily through religious institutions or by governments acting as agents of the church. Book banning and burning has played an important role in European history, such as in France during the Enlightenment, in the USSR during the Bolshevik revolution, and in Germany during the Weimar Republic (Lyons, 2011). There were few laws regulating censorship of information until 1789, when the Constitution of the United States of America was adopted, and individual freedoms, including the right to free speech, became protected. Since then, similar laws have been adopted by other countries around the world (Passavant, 2002).

Today, information has become a digital commodity, and individuals are now limited less by the laws of their home countries and more by international standards. However, no international laws address censorship, and it was only in 2011 that the United Nations Human Rights Council identified unfettered Internet access as a human right (La Rue, 2011). International law regarding information theft lags behind even the UN report, as prosecutions are based on the laws of the countries in which the crimes were perpetrated. Depending upon the country, these laws can be extremely restrictive, very broad, or potentially even in violation of internationally-recognized human rights agreements (La Rue, 2011).

Educational institutions have historically had a special role within society, with libraries and universities acting as both repositories of knowledge and points of information access for their communities. Libraries are common targets for censorship because removing a book from a personal collection blocks access for one person, whereas removing it from the library blocks access for the whole community. As Byrne (2003) notes, librarians cultivate a “professional narrative of non-judgmental, disinterested provision

of access to information” which “confers a legitimacy on their professional choices to make available or not make available” (Byrne, 2003, p. 7). Libraries have historically taken all sides on censorship debates - sometimes removing materials, keeping them in place, or relocating them to special sections. Broadly, though, libraries tend to focus on preserving, protecting, and providing access to information, as can be seen in their central role in preserving culture in locations as varied as Afghanistan and Colombia (Knuth, 2003, 2006).

Censorship in the Modern World

Throughout the modern world, agents of censorship are most commonly either governments or corporations. In countries with laws protecting freedoms of speech, religion, and the press, some acts of censorship are also initiated by individuals. Although China is most commonly associated with censorship, there is widespread agreement that the most restrictive countries in the world are Eritrea, North Korea, Syria, and Iran (Reporters Without Borders, 2013). Other countries, such as China, Ethiopia, Cuba, Saudi Arabia, and Belarus, are also often listed as “most censored” countries, but rankings depend on the perspective of the organization reviewing censorship activities in each nation.

Regardless of the censoring agent, there are three main strategies for censoring materials. The first is removal or blocking of offensive material, which prevents individuals from viewing or experiencing the material at all. As the most common form of censorship, this strategy is typically employed where information is contained within physical artifacts, such as books or recordings. Second, instead of removing the material directly, organizations may instead remove any references to the material, such as a catalog entry or its visibility to a search engine through the use of filters (Zittrain & Palfrey, 2008; Chen & Wang, 2010). With the growth of the Internet and users’ dependence on search engines for finding information, this is often as effective as removing the information entirely. Another variant of this method is blocking certain search terms that may lead to the offensive material, which is the practice used with the Chinese microblogging social media platform Weibo (Ng, 2013). The final method is intimidation. Authoritarian regimes, such as China

or Iran, make it known through a variety of means that exploration of certain materials or ideas is forbidden and may carry consequences for the user. While the ultimate decision to pursue research remains with the user, the disincentive arising from the intimidation may prevent the search from ever taking place.

Due to its rapid growth and power for sharing information, the Internet has recently proven an important battleground for censorship activity. While most Western democracies impose only very limited restrictions on Internet content (such as on child pornography), some developing countries, such as China and Iran, limit access to certain websites or databases (Morozov, 2011). This is accomplished in multiple ways. First, nationally-owned network hardware at the main network connections for the country may be configured to filter out certain websites or information from specific IP address ranges (Joyce, 2010; Yang, 2009). Second, private companies that operate their own servers or networking equipment within the nation may be required to themselves filter or block certain information, websites, or address ranges (Piety, 2012). Finally the nation may actively employ censors who review Internet content, removing or blocking content that is deemed unacceptable (Joyce, 2010; Yang, 2009).

A special challenge posed by the Internet involves its distribution and control. For example, the Internet Corporation for Assigned Names and Numbers (ICANN) coordinates addressing and protocols for communication on the Internet, ensuring the interoperability of communication around the globe (Thierer & Crews, 2003). While ICANN does contain advisors from countries across the world, the corporation is organized as a non-profit in the state of California, and it is not directly answerable to any governmental authority.

On the distribution side, another important consideration is “net neutrality,” or the willingness to pass information to other systems in the global network independent of content, point of origin/destination, or interfacing equipment. While discussions in the United States have primarily been framed in commercial terms, with local Internet Service Providers (ISPs) providing all information equally to their subscribers, there are also significant implications to the free exchange of information worldwide (MacKinnon, 2012). Lack of net neutrality may serve as de facto censorship if users

7 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/censorship-of-digital-resources-worldwide/112628

Related Content

Security of Cloud Computing

Manel Medhioub, Manel Abdelkader and Mohamed Hamdi (2015). *Encyclopedia of Information Science and Technology, Third Edition* (pp. 1493-1501).

www.irma-international.org/chapter/security-of-cloud-computing/112551

Hybrid Computational Intelligence and the Basic Concepts and Recent Advances

Georgios Dounias (2018). *Encyclopedia of Information Science and Technology, Fourth Edition* (pp. 180-190).

www.irma-international.org/chapter/hybrid-computational-intelligence-and-the-basic-concepts-and-recent-advances/183732

Effectively Communicating With Group Decision Support Systems Using Information Theory

Jamie S. Switzer and Ralph V. Switzer (2018). *Encyclopedia of Information Science and Technology, Fourth Edition* (pp. 2121-2131).

www.irma-international.org/chapter/effectively-communicating-with-group-decision-support-systems-using-information-theory/183925

Towards Knowledge Evolution in Software Engineering: An Epistemological Approach

Yves Wautelet, Christophe Schinckus and Manuel Kolp (2010). *International Journal of Information Technologies and Systems Approach* (pp. 21-40).

www.irma-international.org/article/towards-knowledge-evolution-software-engineering/38998

Secure Mechanisms for Key Shares in Cloud Computing

Amar Buchade and Rajesh Ingle (2018). *International Journal of Rough Sets and Data Analysis* (pp. 21-41).

www.irma-international.org/article/secure-mechanisms-for-key-shares-in-cloud-computing/206875