Computers in Human Behavior 29 (2013) 2805–2815

Contents lists available at ScienceDirect

Computers in Human Behavior

journal homepage: www.elsevier.com/locate/comphumbeh

A review of the available content on Tor hidden services: The case against further development

Clement Guitton *

Department of War Studies, King's College London, Strand, London WC2R 2LS, United Kingdom

ARTICLE INFO

Article history:
Available online 14 August 2013

Keywords:
Anonymity
Tor
Hidden services
Unethical content
Censorship

ABSTRACT

Deindividuation theory informs us that anonymity is likely to beget unethical or violent behavior. Since 2002, Tor has implemented hidden services that allow users to host platforms anonymously and these have behaved accordingly with deindividuation theory: the services are used mostly for unethical content. This article realizes the first systematic analysis of users behavior on Tor hidden services. After classifying 1171 services into 23 categories, and carrying out a content analysis of 2165 posts, the article concludes that unethical content is quantitatively and qualitatively more preponderant than ethical content. The advantages of anonymity to store and access this ethical content do not balance the negative impacts caused by the unethical content. Freedom of expression and the lack of censorship, if theoretically praiseworthy, are overshadowed by what users have done with it: using Tor hidden services in unethical ways. Unethical content is undesirable by its very nature of affecting people negatively, which should lead us to reconsider the development of the Tor hidden services. For users simply wishing to stay anonymous and to act ethically, the use of Tor and of web services located in countries with a morally balanced legal system are sufficient. The support for the further development of Tor hidden services should hence stop, which would not hinder the functioning of Tor as an anonymity provider to those needing it.

1. Introduction

In June 2007, Tariq Biasi, 23, blogged criticisms of the Syrian policy on the use of their intelligence services. He argued that Syrian intelligence authorities focused on domestic spying instead of focusing more appropriately on foreign military sources (Spitzer, 2009). Not long later, the Syrian intelligence services arrested and questioned him. They charged him 6 months following his arrest with 'undermining national sentiment' and 'publishing false information' (Spitzer, 2009). A year after his arrest, in May 2008, a court sentenced him to 3 years in prison. The case of Tariq Biasi is not uncommon, and is a reality for many activists who put their life in jeopardy by criticizing the authorities of the country they live in. For activists like Biasi, remaining anonymous can be a matter of avoiding life-threateningconsequences. Furthermore, for many activists, remaining anonymous is not enough; they also need to ensure that their writings will not be suppressed by authoritarian regimes. For instance, in 2010, while Tunisians, Libyans, and Egyptians were successfully toppling their authoritarian regimes, they were circumventing censorship in their own countries by posting on foreign blogs or foreign platforms (Park et al., 2011; Youmans & York, 2012).

To circumvent censorship, bloggers bypassed filters using techniques linked with being anonymous online: a proxy, a secure virtual private network solution, or Tor. Tor, a software which provides non-traceable and anonymous connections, emerged in 2001 from the US government-funded Onion Routing project. The project is well funded ($1.3 million in 2010) with funds from, among others, advocates of free speech such as the International Broadcasting Bureau and Internews Network (Tor Project, 2011). Tor, since 2002, also implements hidden services. Like the web they also allow users to browse pages. But Tor hidden services are quite particular and also different from the web: the servers hosting the content are not locatable, removing all prospects of censorship, and the services guarantee its users' anonymity (Dingledine, Mathewson, & Syverson,2004). Tor hidden services are separate from the software Tor, and Tor can function very well without Tor hidden services. Tor ensures that an Internet user will remain anonymous; Tor hidden services are on the other hand another type of web, with different protocols, protecting the host of content. Tor hidden services are part of the so-called 'deep web', or 'dark web'. Both terms refer to any part of the web not indexed by any search engine on the web. It is therefore difficult to have an overview of the content available on Tor hidden

* Tel.: +44 (0)74 3530 4640.
E-mail address: clement.guitton@kcl.ac.uk

0747-5632/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.chb.2013.07.031

services, which can be advantageous if one does not seek to broadcast their ideas to a large public audience, but which also constitutes a hindrance for researchers.

Following Tor's technical efforts to offer solutions to protect a user's anonymity and to circumvent state censorship, it is fair to ask: What do users do with their anonymity on hidden services? What type of content do users generate? How do they behave on Tor hidden services?

No previous studies have looked systematically at the content available on the Tor hidden services. Opponents to unrestrained free speech often invoke the threats to national security and to the weakest members of society that a complete censor free society represents (Gelber, 2002; Stone, 2009). On the web, threats to individuals and unethical behaviors already take place. For instance slander damaging people's reputation and disturbing their mental equanimity. But victims can at least attempt legal actions as a remedy to remove this damaging content (Levmore & Nussbaum, 2010). With hidden services, this is not possible. In this article, looking at the behavior of individuals acting under the condition of anonymity reveals what users have done with this anonymity. Unfortunately, the study of 1171 sites, and a content analysis of 2165 posts showthat unethical content and behaviors overshadow ethical ones, quantitatively but also qualitatively. The viciousness of stances and content dwarf the low beneficial impact that hidden services have.

This article is divided into four parts. Firstly, the article provides a short literature review that supports the elaboration of two hypotheses the research addresses: content on Tor hidden services relates to challenging the State authority in order to establish a democratic order; and, content on Tor hidden services challenges ethics. Secondly, the methodology is explained. Thirdly, the article presents the results of the research in detail. And fourthly, the article delves into a discussion of the implications of the results for Tor hidden services.

2. Research context and two hypotheses

Hidden services differ from the web technically speaking in two ways: they cannot be shutdown hence preventing censorship, and they guarantee the complete anonymity of the users of the services, unlike the web, as the users use Tor to access the services. On the web, anonymity, understood as the 'noncoordinatability of traits' (Wallace, 1999), is superficial. A trait can be a person's facial features, their name, or their IP address. When these traits are linked together, a person can be recognized and is therefore no longer anonymous. Various agents (e.g. law enforcement agencies and Internet service providers) have the *possibility* to coordinate an IP address to a person's identity. When using Tor, this possibility does not exist. It is not possible to know a user's IP address.

Furthermore, hidden services evade censorship at two different levels. A site on the web has at least two features: the IP address of the server, and the name associated with the IP address. A law enforcement agency wishing to ban or enforce the ban of certain online content can try to bring either of these features down. For the former, the law enforcement agency can first ban the IP address at the level of the Internet service provider. It can also use the IP address to localise the server, and disconnect it or remove the content directly from the server if located within its jurisdiction. For the name associated with the IP address, law enforcement agencies can, again if it is located under its jurisdiction, delete the entry in the authoritative Domain Name Server that a user needs to contact to obtain the match between the name and the IP address. The architecture of the web is hence prone to censorship and hidden services remove these two weaknesses. In Torhidden services, the server hosting the content gives his name generated from its public key to introduction points. These points do not know either the IP of the server or its location, but know the circuit that links to the server. When someone requests the website, the request goes first to a distributed hash table that contains the location (still by circuit rather than by real IP) of the introduction points. The query is then re-routed towards the server. Hidden services hence can prevent anyone from censoring content on them, as it is impossible to know under which jurisdiction the service hosting the service is located. On Tor hidden services, anonymity also means that it is not possible to find the administrator of the service in contrast to the web.

These technical differences between the web and Tor hidden services are critical for a few people. The arrest of the Syrian blogger Tariq Biasi presented in the introduction epitomized what writers and leaders of subversive movements require: an environment free of censorship and where the authors cannot be easily identified if they are located in a country where their writings can put them into jeopardy. Tor hidden services offer such an environment. The first of two hypotheses considered is therefore positive in considering what the development of Tor hidden services brings to society:

H1. Content on hidden services relates to challenging the State authority in order to establish a democratic order.

If the first hypothesis H1 is valid, it will form a strong argument to justify the praiseworthiness of the use of Tor hidden services. Challenging the State's decision without fearing repression is an essential component of democracy, and Tor hidden services would support this purpose. But anonymity, as implemented by Tor hidden services, may further nurture less praiseworthy sentiments within individuals, leading to content of a completely different nature.

Anonymity has two consequences. The first one is to minimize accountability (Wallace, 1999). The second one, less trivial, is to protect informational privacy. Privacy has an inherent value that serves to remove 'pressure to conform', to be free from 'censure and ridicule', 'to promote autonomy' and 'to promote human relations' (Gavison, 1980). People are more likely to conform and to censor themselves when under the watch of others. But the promotion of non-conformity can also result in expressions of values undermining and threatening the weakest members of societies, with hate speech or child pornography surging up on networks. The legal expert Ruth Gavison notes that criminals and con artists need this privacy for their offenses (Gavison, 1980). What are the effects of ensuring the anonymity of usersand non-censurability of material on hidden services?

We have no account of the effects of anonymity on the hidden web or of users' behaviors. On the other hand, accounts exist in the field of psychology of the effects of anonymity on self-interested unethical behavior in laboratory conditions (Nogami, 2009). An unethical behavior is a behavior affecting another individual negatively in their interests, welfare or expectations of others, but it does not have to affect the instigator of the behavior positively (Brass, Butterfield, & Skaggs, 1998, p. 32). A self-interested unethical behavior is on the other hand carried out for the sole purpose of affecting the actor positively in his own interests. In one experiment, the researcher Tatsuya Nagomi tested self-interested unethical behavior with regards to money. She asked four groups of students to flip a coin twice and away from her gaze and to come back totell her the result. She told the first group of students that their results would be identifiable; the second that they would be identifiable and that they would have a reward if they obtained two times tails; the third group that their results would be anonymous; and the fourth one that their results would be anonymous and that they would receive a reward if they obtained two times tails. Both groups that were not identifiable obtained a much