WHAT ARE BOTS AND ARE THEY DANGEROUS TO DEMOCRACY? CURRENT CHALLENGES FOR BOT-RELATED POLICY

The word "bot" is originally derived from the word "robot." Bots have generally been defined as automated agents that function on online platforms.

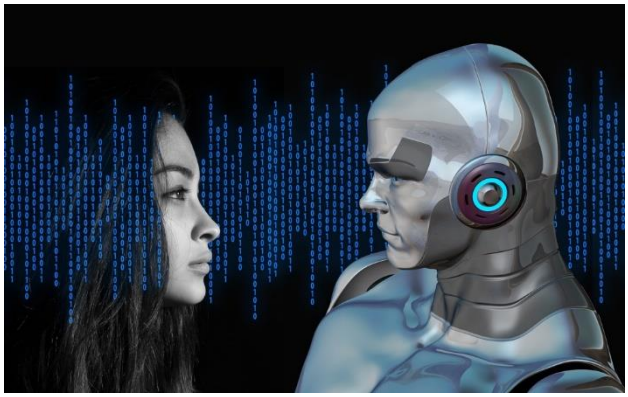


Image source: pixabay.com

However, there is terminological diversity sometimes leading to confusion in this area. The different associated terms include: robots, bots, chatbots, spam bots, social bots, political bots, botnets, sybils, as well as cyborgs, web scrapers, crawlers, indexers, interactive chatbots that interact with users via a simple text interface, and the simple autonomous agents that played a role in early online "multi-user dungeon" (MUD) games.

We are interested here primarily in **chatbots** - a form of human–computer dialog system that operates through natural language via text (Facebook Messenger, Skype, Slack, WeChat, Telegram) or speech (Apple's Siri and Amazon's Alexa), as well as in **social bots** - automated accounts that produce content and interact with humans on social media.

In between, there are 'VTubers' – virtual, animated versions of YouTube's human influencers.

Bots, especially social bots are often used for malicious purposes, including spreading spam and malware links. Social bots that are deployed for political purposes are known as **political bots**. Those political bots that describe fake identities used to interact with ordinary users on social networks, especially when coordinated by government proxies or interrelated actors, are called **trolls**. In some countries and in journalism "troll" and "bot" are generally seen as interchangeable terms, and indicate content manipulation without regard to automation. In the Digital Forensic Research Lab. they distinguish trolls from other accounts based on their aggressive and offensive language.

Close to chatbots and social bots are **spambots**, i.e. computers or other networked devices compromised by malware and controlled by a third party. Spambots post on online comment sections, and can spread advertisements (including fake) or malware on social media platforms. Those spambots that spread commercial or malicious content in some cases may differ from social media bots only in terms of their use.

While some social media bots, like those on Twitter, can occasionally feature chatbot functionality that allows them to interact directly with human users, most chatbots remain functionally separate from typical social media bots. **There are some checklists that may help to identify real and fake bots.**[1]

The current challenges with blogs were enabled by open application programming interface (API) and policies that encouraged developers to creatively deploy automation through third party applications and tools – typically in case of Twitter. Moreover, current methods for Twitter bot detection are not able to accurately detect cyborg accounts (which exhibit a combination of automation and of human curation), as any level of human engagement is enough to throw off machine-learning based models based on account features.

Why and How Should Bots Be Regulated?

Bots are responsible for significant proportions of online activity, are used to game algorithms and recommender systems, can stifle or encourage political speech, and can play an important role in the circulation of hyperpartisan "fake news". Social bots can be used both for commercial and political purposes, as well as for search engine optimization, spamming, and influencer marketing. Bots can contribute to misinterpretation of social data analysis.[2]

As put by Chaurasia (2018):

1) There should be a regulation for businesses to declare their intended use of AI bots (those enabled with natural language processing technology that allows to respond to tweets, or messages). It is **the user's right to know whom they are speaking to.**
2) Moreover, there is a need for strong policies **protecting the security and privacy of private data.** These policies should entail directives regarding what data to collect and why the users should be made aware of them in advance. These policies should be included in the privacy policy statement and the users should be given sufficient time to read it. Additionally, the chatbots should also enable the user to store, encrypt, retrieve, and erase their personal data.
3) Since rogue chatbots are emerging as one of the biggest threats from AI, **a strong framework to prevent or at least minimize negative scenarios is in need.**

[1] So lassen sich Social Bots enttarnen (2017, July 14), http://www.bpb.de/252589/social-bots-enttarnen

[2] Social Bots – die Technik hinter Fake-News (25.04.18), https://www.ionos.de/digitalguide/online-marketing/social-media/social-bots-was-koennen-die-meinungsroboter-wirklich/

4) The authorities need to ensure **to regulate any promotional information** the users are getting through the bots.

5) **Terms and Conditions** should be presented to the users in a clear manner and the bot should be able to transfer the issue on T&Cs to the human support as any unintentional or accidental claim by the bots may also become a part of T&Cs. It is also important to ensure that whatever information T&Cs contain should be in accordance and compliance with regulatory policies.

6) In order to guarantee **protection of minors**, regulation should guarantee the bot's ability to verify age and tailor content.

7) It should be considered whether the bots should start **handling moral duties and responsibilities**. A regulatory arrangement around this is important as to whether the bots should call for a human help or apprise the authorities in situations that indicate a sign of threat to life or breach of law and order. This question should also have a clear answer in company policies.

Lamo and Calo (2018, 36-37) suggest (more from a US freedom of speech perspective) the following regulatory choices:

First, governments should begin by updating and leveraging **existing law to address harms caused by bots**.

Second, governments should regulate bot speech, if at all, **through individual restrictions aimed at (i) particular categories of bots, (ii) within specific contexts, and (iii) supported by concerns/examples about the specific harms the government hopes to mitigate**.

Governments should in all instances interrogate whether their proposed solution sweeps in harmless speech and, conversely, whether it actually addresses the harmful activity at issue. The governments should acknowledge that, for at least some categories of bot speech, the requirement to self-identify itself operates as a restriction on expression.

Third, governments should anticipate and address **inevitable issues around enforcement.** With respect to a generic bot disclosure law, there will be many instances in which an official or citizen suspects non-compliance. Such a path could include **a means by which the platform or another third-party can verify the human nature of a given account, or provide penalties for attempting to silence an individual by falsely reporting her to be a bot.**

Fourth, governments should acknowledge the downstream effects of officially differentiating between bot speech and other forms of online communication. In theory, bot disclosure laws merely offer signals to individuals as they navigate a complex information ecosystem. But in practice, those signals may come to serve as the scaffolding for private or, outside of jurisdictions with a robust free speech tradition, public censorship of bots as a category of speech. The question is under what conditions governments can, or at any rate should, alter the character of speech to make it more susceptible to various forms of suppression, conclude Lamo and Calo (2018).

Regulatory Suggestions

Mukkadam (2017) identified the following legal issues related to chatbots:

Table 1: A summary of the key legal issues to be considered with regard to chatbots

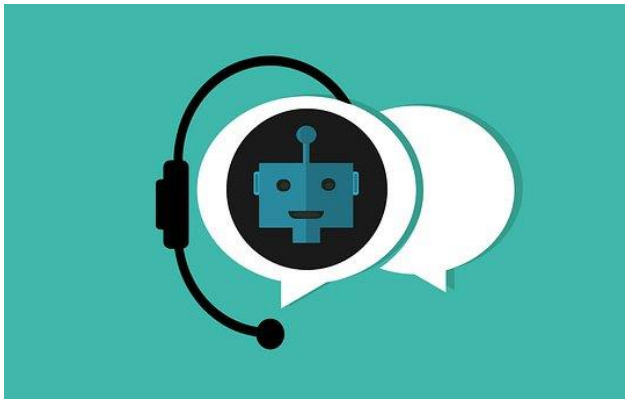
Regulatory Issue	Suggested Approaches
Policies on chatbots	Internal policies must be in place which govern the extent of the chatbot's permitted activities, information that it will be fed, information it will collect and where that information is stored/sent, and all ancillary policies must be reviewed to make provision for chatbots if appropriate.
Website T&Cs and disclaimers	Depending on the type of activity that is being carried out by the chatbot, consideration should be given to whether reference to the chatbot is made in the website/platform T&Cs and if appropriate disclaimers are required.
Regulated industries/activities	Where chatbots are used in regulated industries, the activities of the chatbot must be programmed to comply with industry regulations and standards. Where a chatbot is giving advice for instance, information fed to the chatbot must be kept up to date. Appropriate escalation measures need to be in place and disclaimers should be considered. Similarly, where chatbots are used for regulated activities, for example advertising, chatbots will need to be programmed to comply with the relevant regulations. Appropriate oversight must be in place.
Data collection	Data controller registrations and privacy policies must be up to date; it must be clear where the data is collected and where it will be processed, the relevant controller-processor agreements (if required) must be in place to govern the transfer of any data outside of the EEA, technological protection measures must be in place to safeguard data, and data privacy policies must be up to date
Defamation/abuse/ harassment	Where chatbots are used to stimulate conversation, appropriate measures must be in place to prevent the chatbot's comments going too far and straying into the territory of libellous comment, abuse or harassment.
Infringement of third party rights	Appropriate safeguards must be in place to prevent infringing copyright protected content, using third party trademarks and brands, linking to information/content behind paywalls, or otherwise'screen scraping' where information from third party sources is extracted and re-utilised by the chatbot.
Policy on monitoring/ human intervention trigger	Consideration should be given to the extent of monitoring of chatbot's activities and a human intervention trigger must be in place to prevent things going too far.

It should be mentioned that **there are already some policies** in place. The key social media platforms such as Twitter, Instagram and Facebook clearly mark original accounts. Moreover, they limit number of followers and/or followed accounts. Finally, platforms regularly report deletion of a large number of fake accounts (bots).

In a related move, **the European Parliament has voted to outlaw the use of automated ticket-buying software or ticket bots** in early 2019. Ticket bots enabled touts to bulk buy concert tickets and resell at inflated prices.

Gorwa and Guilbeault (2018) suggest that policy at both the industry and public level will need **to be designed differently to target "bots" with different structural characteristics**. For example, if policy makers are particularly concerned with bots that rely on API access to control and operate accounts, then **social media companies should impose tighter constraints on their API as an effective redress.** It appears as if most of the Twitter bots that can be purchased online or through digital marketing agencies are built to rely on the public API, so policy interventions at this level are likely to lead to a significant reduction in bot activity.

Second, questions concerning the function of a bot are essential for **targeting policy to specific kinds of bots**. For example, social bots, which communicate primarily over public posts that appear on social media pages, are typically built to rely on hard-coded scripts that post predetermined messages, or that copy the messages of users in a predictable manner.



The third category specifically refers to how the bot is used, and what the end goal of the bot is. This is arguably the most important from a policy standpoint, as it contains ethical and normative judgements as to what positive, acceptable online behavior is. The challenge for policymakers trying to regulate bots is that structurally, the same social bots can simultaneously enable a host of positive and negative actors. **Any regulation on bots, either from within or from outside of social media companies, would need to distinguish types of bots based on their function in order to formulate clear regulations to address the types of bots that have negative impact, while preserving the bots that are recognized as having a more positive impact. It may be most useful to develop regulations to address social bots**. In general, **automation policies—like other content policies—should be made more transparent,** or they will appear wholly arbitrary or even purposefully negligent.

Any initiatives suggested by policymakers will have to deal with several pressing challenges. On the one hand, there is conceptual ambiguity. For example, it is not always easy to track what is commercial or political communication, especially when bots can generate unpredictable text (Lamo and Calo, 2018).

On the other hand, there is poor measurement and data access, lack of clarity about who exactly is responsible, imperfect bot detection methods, an overall lack of reliable data and the overarching challenge of business incentives that are not predisposed towards resolving the aforementioned issues.

This part was reviewed by Nika Aleksejeva (University of Latvia and currently working for NATO Strategic Communications Centre of Excellence in Riga, Latvia) and by Lukasz Porwoll, Insight Institute, National University of Ireland, Gallway, Ireland.