Date of Hearing:

ASSEMBLY COMMITTEE ON ARTS, ENTERTAINMENT, SPORTS, TOURISM, AND INTERNET MEDIA
Kansen Chu, Chair
SB 1001 (Hertzberg) – As Amended June 21, 2018

SENATE VOTE: 26-10

SUBJECT: Bots: disclosure.

SUMMARY: This bill would make it unlawful for any person to use a bot, as defined, to communicate or interact with persons in California online, with the intention of misleading for specified purposes, and without clearly and conspicuously disclosing that the bot is not a natural person, as specified. Specifically, **this bill**:

1) Declares that it shall be unlawful for any person to use a bot to communicate or interact with another person in California online, with the intent to mislead the other person about its artificial identity for the purpose of knowingly deceiving the person about the content of the communication in order to either:

    a) Incentivize a purchase or sale of goods or services in a commercial transaction, or;

    b) To influence a vote in an election.

2) Provides that a person using a bot shall not be liable under this section if the person discloses that it is a bot.

3) Further provides that the disclosure required by this section shall be clear, conspicuous, and reasonably designed to inform persons with whom the bot communicates or interacts that it is a bot.

4) Contains the following definitions:

    a) "Bot" means an automated online account on an online platform that is designed to mimic or behave like the account of a person.

    b) "Online" means appearing on any public-facing Internet Web site, Web application, or digital application, including a social network or publication.

    c) "Online platform" means any public-facing Internet Web Site, Web application, or digital application, including a social network or publication.

    d) "Person" means a natural person, corporation, limited liability company, partnership, joint venture, association, estate, trust, government, governmental subdivision or agency, or other legal entity or any combination thereof.

5) Provides a severability clause, as specified, and states that the duties and obligations imposed by this chapter are cumulative with any other duties or obligation imposed by any other law.

EXISTING FEDERAL LAW:

1) Provides, under the U.S. Constitution, that "Congress shall make no law . . . abridging the freedom of speech, or of the press, or the right of the people peaceably to assemble, and to petition the government for a redress of grievances." (U.S. Const., 1st Amend., as applied to the states through the 14th Amendment's Due Process Clause; *see Gitlow v. New York* (1925) 268 U.S. 652.)

2) Provides as a matter of federal case law that the government may not, under the First Amendment to the United States Constitution, suppress political speech on the basis of the speaker's corporate identity. (*Citizens United v. FEC* (2010) 130 S.Ct. 876.)

EXISTING STATE LAW:

1) Provides under the California Constitution for the right of every person to freely speak, write and publish his or her sentiments on all subjects, being responsible for the abuse of this right. Existing law further provides that a law may not restrain or abridge liberty of speech or press. (Cal. Const., art. I, Sec. 2(a).)

2) Prohibits any person, firm, corporation or association, or any employee thereof, from making statements that are untrue or misleading in connection with communications regarding the sale of goods or services, including over the Internet. (Business and Professions Code (BPC) Section (§) 17500)

3) Prohibits a person, with a bad faith intent, to register, traffic in, or use a domain name that is identical or confusingly similar to the name of another living or deceased person. (BPC § 17525)

4) Prohibits any person or entity from sending a commercial e-mail advertisement from California or to a California electronic mail address if the e-mail advertisement contains falsified, misrepresented, or forged header information or if the e-mail advertisement has a misleading subject line. Permits the AG, among other parties, to bring action against a person or entity that violates these provisions. (BPC §17529.5)

5) Prohibits a person or entity located within California from using a telephone facsimile machine, computer, or other device to send an unsolicited advertisement to a telephone facsimile machine. (BPC § 17538.43 (b)(1))

6) Requires a person or entity located in California to clearly mark the date and time of transmittal and identity and telephone number of the person or entity sending the message of any communication via a telephone facsimile machine. (BPC § 17538.43 (c)(1))

7) Requires individuals or partnerships doing business under fictitious names to file a fictitious business name certificate designed to make the identities of the persons doing business under the fictitious names available to the public. (BPC § 17900)

FISCAL EFFECT: According to the Senate Appropriations Committee, pursuant to Senate Rule 28.8, any additional state costs are not significant, and do not and will not require the appropriation of additional state funds, and the bill will cause no significant reduction in revenues.

COMMENTS:

1) *Author's and supporter's statement of need for legislation:* According to the author, "there is currently no law that relates to the disclosure of the use of bot accounts on social media. SB 1001 sheds light on the fake accounts that simulate real people and spread waves of false information across social media platforms. On the Internet where the appearance of a mass audience can be monetized, it is critical to protect users by providing the tools to understand if their information is coming from a human or a bot account disguised as one. As long as bots are properly identified to let users know that they are a computer generated or automated account, users can at least be aware of whom they are interacting with and judge the content accordingly."

   Common Sense Kids Action is the sponsor of SB 1001. They write the committee to share their belief that, "American democracy and civic discourse in 2018 remain under attack from bots and disinformation." Adding, "(A)s the advocacy arm of Common Sense Media, Common Sense Kids Action works to ensure that children can thrive in today's digital world. Sixty-six percent of American teens use Facebook, 47% use Twitter, and 39% say social media is their preferred news source. They are at risk with being targeted with unlabeled bots on those platforms, which have an estimated 60million (Facebook) and 48 million (Twitter) unlabeled bot accounts. …With so many kids online; families need confidence that they will be protected from unlabeled accounts that are spreading false information and harmful content." In order to demonstrate the havoc bots can wreck, the sponsors shared the following list of articles and accounts of the impact bots have on the online world:

   - *Expert: Bots are poised to wreak havoc in the 2018 midterm elections*. Samuel Woolley a technologist in Palo Alto reports that in "almost any" election happening in America in 2018, you see evidence of bots being used to manipulate the vote.

   - *Mueller warns that election, politics meddling by foreigners is still happening*. In June of 2018, Special Counsel Robert Mueller informed the United State District Court of ongoing Russian election interference, following the patterns of bots and disinformation from 2016.

   - *Bots Hosted by American Social Media Platforms interfere with Mexico's Election*. Mexico has long faced some of the worst human rights and democracy abuse by bots, and it is continuing in the 2018 elections.

   - *Unilever gets serious about influencer fraud.* One of the world's largest advertisers is rethinking its exposure to social media platforms populated by unlabeled bots that are taking advantage of public trust.

2) *Background.*

a) *The use and misuse of bots.* According to research conducted by the Center for Complex Networks and Systems Research at Indiana University and the Information Sciences Institute at the University of Southern California, "[i]ncreasing evidence suggests that a growing amount of social media content is generated by autonomous entities known as social bots." (Onur Varol, et al., *Online Human-Bot Interactions: Detection, Estimation, and Characterization* (Mar. 27, 2017). Their estimates suggest that as many as 15 percent of Twitter accounts are fake. This would mean roughly 48 million Twitter users are bots, automated to simulate real people. Facebook itself disclosed to its investors that the social media platform had "at least twice as many fake users as it previously estimated, indicating that up to 60 million automated accounts may roam the world's largest social media platform." (Confessore, et al., *The Follower Factory* (Jan. 27, 2018) The New York Times.

As explained by the Senate Committee on Business and Professions, Bots are software applications that run automated tasks on a network, such as the Internet, that can interact with computers systems or users. Bots can be purchased or created by individuals or organizations and many online platforms, including social media sites, create bots themselves and encourage users to build bots for use on their platforms. There are a variety of different types of bots that are programmed to perform different tasks. Examples include search engine crawler bots, such as GoogleBot or BingBot, that help search engines discover new content; copyright bots, such as YouTube Content ID, that help identify content posted online that violates copyright law; and chatbots that are designed to simulate conversations with human users, often in order to perform tasks such as booking a flight. Some types of bots are created with malicious intents, including scraping content, stealing passwords, spamming websites, or scalping tickets.

When interacting directly or indirectly with bots online, human users may not be able to discern if they are interacting with a bot or another human. For example, human users on a company's customer support system may assume they are communicating directly with a human customer service employee, but instead are texting with a bot. Similarly, human Twitter users may assume a Tweet was posted by another human when in actuality the content was generated by a bot. The latter type of interaction has become increasingly common as the number of automated users on social media sites continues to grow.

Bots that are automated accounts on social media sites can be used to amplify the perceived popularity of people, products, and services online. In January 2018, the *New York Times* published an article, "The Follower Factory," detailing an emerging market where those seeking to bolster their online presence can purchase followers, likes, and other engagements for their Facebook, Twitter, LinkedIn, YouTube, and other social media accounts from companies that control a large number of bots. One such company highlighted by *The Times*, Devumi, has reportedly sold Twitter followers to over 200,000 customers, including reality television starts, professional athletes, and politicians. To do so, Devumi draws upon its approximately 3.5 million bot accounts, at least 55,000 of which use the names, profile pictures, and other personal details of real Twitter users. Since a higher follower count implies a higher popularity or importance of the person or product, purchasing followers from companies like Devumi can lead to a real increase in human users engaging with the purchasers account and even lead to endorsement deals

from companies seeking to capitalize on a user's perceived online influence. Social media platforms use similar metrics to determine the popularity of an account, which can influence which accounts a platform recommends or which posts a platform determines are trending.

Just as companies like Devumi use bots to promote their customer's accounts, individuals and groups can, and have, used bots to spread and amplify divisive views on social media platforms. In February 2018, the U.S. Justice Department charged 13 Russians and three companies with creating fake profiles on social media sites to post contentious comments related to religion, race, and politics and then using bot accounts to like, share, and retweet the posts to help them gain traction. Information provided to U.S. Congress on October 20, 2017 indicated that Russian agents published more than 131,000 messages on Twitter, uploaded over 1,000 videos to YouTube, and disseminated inflammatory posts that reached 126 million users on Facebook.

b) *Regulation and legislation of bots*. Many online platforms have their own policies regarding the use of bots, including Twitter which introduced new policies regarding the use of automated accounts in February 2018. While bots are still allowed on Twitter and developers are still encouraged by Twitter to create useful bots that add to the platform's online community, individuals are now prohibited from using "any form of automation…to post identical or substantially similar content or perform actions such as Likes or Retweets across many accounts." Twitter also has a variety of enforcement mechanisms in place, including requiring an account suspected of violating its policies to verify ownership with a phone number or email address. Twitter states that this enforcement mechanism helps it "identify violators who are operation multiple accounts for abusive purposes and take action on such accounts." As its most severe enforcement action, Twitter permanently suspends accounts. Users can appeal permanent suspensions through the platform interface or by filing a report but it is unclear exactly how long Twitter's investigative and enforcement process takes.

There have recently been efforts by other states and the federal government to regulate the use of bots and prevent the spread of misinformation and false advertising by automated accounts. In 2016, President Obama signed the Better Online Ticket Sales Act, or BOTS Act, (2016; 114th Congress S. 3183) which prohibited the use of bots to scalp tickets by automatically purchase event tickets online and reselling them on secondary ticket-selling websites at a significantly higher price. This year, legislators in several states, including New York, Maryland, and California, as well as the U.S. Congress, have introduced legislation to regulate the purchasing of social media advertising, including by bots. However, there is currently no state that requires the disclosure of bots.

3) *Recent amendments remove opposition – however discussions continue on potential clarification of "clear and conspicuous" disclosures*. The author accepted narrowing amendment in the Assembly Committee on Privacy and Consumer Protection which removed opposition of the coalition of California business and technology organizations. There were however lingering concerns over the legal standards for what is "clear and conspicuous," which vary from mobile platforms to internet based sites. While these concerns do not rise to the level of opposition, the coalition remains in talks with the author about addressing challenges to implementation of this language.

There is guidance for the coalition, found in Federal Trade Commission (FTC) standards for online advertisements, and their views on what constitutes a clear and conspicuous disclosure on various platforms, and even sites such as Twitter and Instagram. As explained in the article, *Clear & Conspicuous': What It Now Means to the FTC in Digital Advertising*, Rothbard, (2013), "The revised guidelines make clear that FTC truth-in-advertising principles apply to any medium, platform or device – no matter how new or small – and attempt to offer practical advice for complying with FTC disclosure requirements in online, social media and mobile advertising.

"What will make a disclosure "clear and conspicuous" in a digital ad? The FTC's criteria are:

- Placement and prominence of the disclosure and how close it is to the related claim;
- Whether the disclosure is unavoidable;
- Whether other parts of the ad distract from the disclosure;
- Whether the disclosure needs to be repeated to ensure it's seen; and
- Whether the language is understandable.

"The revamped guide also strongly discourages scrolling to find a disclosure, especially horizontal scrolling on smaller screens which consumers rarely do (any need to scroll horizontally can be solved by having a mobile-optimized site). When scrolling can't be avoided, effective text or visual cues need to lead consumers to the disclosure. Pop-ups are another FTC disclosure non-favorite since they can be easily blocked and are often ignored.

"Where space constraints are acute, such as in tweets, the revised guidance encourages repetition of disclosures (such as republishing in 're-tweets') and allows abbreviated disclosures as long as consumers understand them. For example, 'Ad' should be adequate to indicate a tweet is sponsored, but not necessarily '#spon.'"

4) *Constitutional concerns remain despite narrowing of legislation.* The Assembly Committee on Privacy and Consumer Protection analysis of this bill contains an exhaustive discussion of constitutional principles and concerns raised by this bill. (Please see their committee analysis for more a in depth discussion). The recent amendments have taken care of many issues, but not all. In the final analysis it will be up to a court to determine if the measure passes constitutional muster. The following is a summary of issues raised by this measure as discussed in their analysis.

This bill would declare it to be a violation for any person (meaning both natural persons and corporations or other legal entities) to use a bot, as defined, to communicate or interact with persons in California online, with the intention of misleading a person about its artificial identity. Under this bill, a person using a bot would be presumed to not act with the intent to mislead if the person discloses that the bot is not a natural person.

Fundamentally, this bill, like others brought before the Legislature this year, triggers a debate surrounding the First Amendment issues implicated by bot regulations. As a matter of constitutional law, even if bots do not directly have speech rights, they are connected to individuals (or corporations) who do. Indeed, bots do not appear out of thin air; they are created by a natural person or entity for a purpose. Namely, they enable the creator to associate themselves with the bot's "speech," or rather, to express themselves, or speak,

through the bot. Bot accounts on social media can have legitimate and beneficial uses, let alone less favorable but still constitutionally-protected ones. The content produced by bots on behalf of the speaker arguably does not lose its First Amendment protection merely because it is "spoken" through a bot.

That being said, not all speech is always protected speech: the First Amendment reflects a fundamental right protecting the freedom of speech and expression; it is not an absolute right. The determination about whether a specific statute inappropriately restricts speech can vary depending on whether the content regulated is a lesser protected type of speech. For example, speech that falls under the category of obscenity or incitement is not afforded the same protections as conversational speech about current events or religious speech or artistic expression. Nor is commercial speech afforded the same protection as political speech. The latter categories receive greater scrutiny in analysis and require a demonstration that the laws are sufficiently narrowly tailored to achieve a compelling governmental interest. Ultimately, when conducting a constitutional analysis of government restrictions on freedom of speech, the analysis invariably requires a determination as to whether the restriction is content-neutral or content-based; unduly vague or overbroad; and whether the restriction acts as a prior restraint on speech. At times, questions around government regulations may also relate to whether the statute unconstitutionally prohibits anonymous speech, or actually compels speech, as the First Amendment also protects the right to speech anonymously, and the right to stay silent.

Here, the question becomes whether this bill meets such constitutional standards, particularly as the underlying premise of this bill appears to be that any and all speech expressed by way of a bot is less trustworthy (or constitutes a fact that is relevant to its trustworthiness), or will inherently mislead people if the identity of the bot "speaker" is left undisclosed.

5) *Prior and related legislation*:

a) AB 1950 (Levine) Legislation of 2018, as introduced, would have prohibited an operator of a social media site with a physical presence in California from selling advertising to a computer software account or user that performs an automated task and is not verified as being controlled by a natural person. Status: That bill was later gutted and amended into a bill related to the California Online Protection Privacy Act and was held in Assembly Committee on Privacy and Consumer Protection.

b) AB 3169 (Gallagher), Legislation of 2018, would have prohibited any person who operates a social media internet website or search engine located in California, as specified, from removing or manipulating content on the basis of the political affiliation or political viewpoint of that content. Status: The bill failed passage in Assembly Committee on Privacy and Consumer Protection on April 3, 2018.

c) AB 1832 (Calderon), Chapter 158, Statutes of 2014, expanded the provisions of AB 329 (Pan) which prohibited the intentional use or sale of software to circumvent a security measure, access control system, or other control or measure used to ensure an equitable ticket buying process, to any platform and not only on a ticket seller's Internet Web site.

d) AB 329 (Pan), Chapter 325, Statutes of 2013, made it a misdemeanor to intentionally use or sell software to circumvent a security measure, access control system, or other control

or measure on a ticket seller's Internet Web site that is used to ensure an equitable ticket buying process.

REGISTERED SUPPORT / OPPOSITION:

Support

Common Sense Kids Action (Sponsor)

Opposition

None on file

Analysis Prepared by: Dana Mitchell / A.,E.,S.,T., & I.M. / (916) 319-3450