22 Vand. J. Ent. & Tech. L. 839

Vanderbilt Journal of Entertainment and Technology Law
Summer, 2020

Article

Barry Stricke[a1]

PEOPLE v. ROBOTS: A ROADMAP FOR ENFORCING CALIFORNIA'S NEW ONLINE BOT DISCLOSURE ACT

Abstract

Bots are software applications that complete tasks automatically. A bot's communication is disembodied, so humans can mistake it for a real person, and their misbelief can be exploited by the bot owner to deploy malware or phish personal data. Bots also pose as consumers posting online product reviews or spread (often fake) news, and a bot owner can coordinate multiple social-network accounts to trick a network's "trending" algorithms, boosting the visibility of specific content, sowing and exacerbating controversy, or fabricating an impression of mass individual consensus. California's 2019 Bolstering Online Transparency Act (the "CA Bot Act") imposes conspicuous disclosure requirements on bots when they communicate or interact with humans in California. Call it Isaac Asimov's fourth Rule of Robotics: A robot may not pretend to be a human being. *By requiring bots to "self-identify" as such, the CA Bot Act is a pioneer in laws regulating artificial intelligence. Most of its criticism points to the act's lack of an enforcement mechanism to incentivize compliance. Accordingly, this Article lays out a map to sanction violations of the act with civil actions under California's Unfair Competition Law and statutory tort law of fraudulent deceit. It outlines what is prohibited, who can be sued, and who has standing to sue, then addresses First Amendment limits on unmasking John Doe defendants via subpoena. For many reasons, attempts to hold CA Bot Act violators liable are most likely to prevail in the commercial arena. But a willful use of bots to undermine a political election or prevent voting might also be a worthy target. Ultimately, the law could be strengthened with an articulated enforcement provision. But if the CA Bot Act aims a first salvo against malicious online bots, this Article hopes to spark the powder.*

***840 Table of Contents**

***841 I. Introduction**

On September 28, 2018, Governor Jerry Brown signed into law California Senate Bill 1001, the so-called Bolstering Online ***842** Transparency Act (the "CA Bot Act").[1] Bots (short for "robots"),[2] are software applications that complete tasks independent of human control.[3] Under the CA Bot Act, online bots that try "to incentivize a ... commercial transaction or to influence a vote in an election"[4] must now disclose they are bots to California residents.

The CA Bot Act is among the first US laws to regulate online artificial intelligence (AI)[5] and the first to require bots to "self-identify" to humans. The use of deceptive online bots is allegedly widespread,[6] and enforcing the act may have significant implications for a variety of stakeholders.

Through their ability to act and respond independently, bots can mimic the behavior of real people.[7] Since their communication is disembodied, bots can effectively fool people into believing the bots are actual humans conversing. The humans' mistaken belief can be exploited for malicious ends, like gaining trust and access to a user's private information. In fact, so-called chatbots, which converse via natural-sounding language, are typically evaluated by their ability to convince people that the bot is a fellow human.[8] Therein lie the origins and controversy of the CA Bot Act.

Commercially, bots play an ever-growing role, particularly in customer service.[9] Politically, federal and state government ***843** investigations[10] evidently confirm many researchers' beliefs[11] that bots routinely manipulate the online exchange of information for commercial and political purposes.

And yet despite their well-earned stigma for malicious activity, bots range widely in purpose and sophistication, and many perform tasks that are benign or beneficial, like indexing the internet's vast data or interpreting online inquiries to reply with relevant information.

Both the act's legislative history[12] and public comments by its sponsor, Senator Robert Hertzberg,[13] illustrate efforts to preserve bots' utility: tailoring the definition of "bot"; removing a prior presumption of the bot owner's intent to mislead; instead requiring an intent to deceive be shown; requiring only disclosure that a bot is a bot; and adding language to narrow which speech is covered by the act.[14]

Likely the most contentious element of the original legislation was its notice-and-takedown system, obliging online publishers to suspend suspected bot accounts in response to a user complaint pending an investigation.[15] The federal Digital Millennium Copyright Act (DMCA) polices online copyright infringement with a similar scheme,[16] much criticized for its abusers' stifling of online speech, and free-speech advocates successfully had the clause removed from the CA Bot Act.[17] ***844** As adopted, the law reverses direction, explicitly exempting internet service providers (ISPs) and social networks from *any duties* under the act.[18]

That said, while the CA Bot Act removes *liability* from social media providers, they can be subpoenaed to unmask bot owners;[19] Part IV discusses when such subpoenas may be enforced.[20]

The CA Bot Act is mute on both criminal and civil enforcement. To date, the California Department of Justice and the California attorney general have not issued an opinion on the new law.[21]

Notwithstanding this eventuality, a *private* actor can seek redress for CA Bot Act violations under California's Unfair Competition Law (the UCL)[22] and California's statutory tort of fraudulent deceit.[23] Both legal frameworks would require the plaintiff to allege and prove the act has been violated.[24] Thus, Part II of this Article examines which bots may be subject to CA Bot Act, what bot behavior may violate it, and what might constitute adequate disclosure. Part III explores the issues of causation, harm, and remedies in a variety of prospective civil actions to sanction CA Bot Act violators. Part IV discusses anonymous speech and First Amendment restraints on subpoenas to unmask online speakers. This Article concludes that an individual or class action to sanction violations of the CA Bot Act is not only feasible but could be won, thereby unmasking, punishing, and deterring the fraudulent use of bots by drawing blood, perhaps even through a class action with punitive damages.

***845 II. Which Bots Have to Disclose (and How)?**

Since its inception, the internet has confounded attempts at regulation, transcending well-established boundaries of the physical world to upend traditional legal principles governing contracts,[25] real property,[26] civil procedure,[27] intellectual property,[28] employment,[29] defamation,[30] and discrimination.[31] Early encounters by courts with new technologies[32] have led to decisions that have been criticized as profoundly misunderstanding the technology.[33]

The CA Bot Act may have avoided that pitfall; it seems drafted with restraint and a comprehension of how bots function. The law's "bot" definition is narrowed to preserve the utilities of software automation. The act is not violated without an intent to

deceive online users, thus guarding against benign and beneficial bots being sanctioned as a result of inadvertent confusion. Bot owners' speech and activity remain fundamentally untouched, provided they disclose that a bot is being used to do the speaking and acting. And the act targets only the bot speech raising the most social concern: misleading ***846** communication directed at making a sale or influencing political elections. Even the law's critics acknowledge the act's laudable goals and the challenges of prohibiting malicious bots.[34]

With that in mind, Part II examines what kind of bot communication would be deemed illegal under the CA Bot Act, thereby triggering its disclosure requirement. This Part employs a taxonomy of online bots to explore the act's definition of "bot" and its elements: (i) communication with a person online, (ii) intent to deceive the person about the bot's nature, (iii) knowledge of the person's misbelief, and (iv) a purpose to either "incentivize" a commercial transaction or "influence" an election vote. By design, the most salient defendants for a successful and worthwhile civil action under the CA Bot Act are its intended targets, "social bots," which obtain and develop online profiles and behave like humans, posting and reposting media, messaging, and commenting and evaluating content--all in order to trick humans into making a commercial transaction or deciding how to vote in an election.[35]

A. Interpreting the CA Bot Act's Statutory Language

The CA Bot Act makes it unlawful for any person to

> use a bot to communicate or interact with another person in California[36] 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 incentivize a purchase or sale of goods or services in a commercial transaction or to influence a vote in an election.[37]

A second clause removes liability if the bot discloses in a manner that is "clear, conspicuous, and reasonably designed to inform persons with whom [it] communicates or interacts that it is a bot."[38]

***847** This construction poses a threshold question: Is *non-disclosure* an *element* to allege and prove, or is *disclosure* an *affirmative defense* that the defendant must raise?[39] If it were an element, and the California attorney general sought to impose civil penalties on violators,[40] the government would have the burden of proof to show insufficient disclosure,[41] particularly since the CA Bot Act likely implicates speech, making the state's burden to justify penalizing conduct more pronounced.[42]

The prohibition of bots and the disclosure "immunity" are distinct sentences in the CA Bot Act, perhaps pointing to disclosure being an affirmative defense. On the other hand, they are placed in the same legal clause, suggesting that nondisclosure is an element. In any case, it may not matter to either of the two available civil frameworks to sanction a CA Bot Act violation, since both require proving that the act was violated. Accordingly, this Article treats nondisclosure as an element under the CA Bot Act.

B. What Constitutes a Bot Under the CA Bot Act?

The CA Bot Act's legislative history[43] and sponsor[44] attest to the challenge of defining a "bot" for regulation. Bots generally include software that completes a task automatically, like replying to email ***848** while the user is out of town.[45] The CA Bot Act narrows this, defining a bot as an "automated online account where ... substantially all of the actions or posts of that account are not the result of a person."[46]

Thus, leaving aside academic debates asking if any computer activity is "not the result of a person,"[47] it appears that occasionally employing autoreply software on an email account would not make it a bot under the statute, whereas deploying automated software on an email account used *exclusively* to communicate with human recipients might very well meet the CA Bot Act's definition.

C. Which Bot Behavior Triggers the CA Bot Act's Disclosure Requirement?

1. The CA Bot Act Regulates Bots that Talk to People

The California legislators' attempt at restraint is also evident in the fact that the CA Bot Act does not prohibit or impose disclosure requirements on *all* bot activity. For example, the act governs only bot owners[48] using bots to "communicate or interact"[49] with another person.[50] Evidently unaffected are bots that communicate with a computer or other bots. Clarifying the distinction will tease out some of the legal questions raised by any effort to sanction bot owners under the CA Bot Act.

849** ***a. Bots that Talk to Computers: Spiders, Crawlers, and Web Scrapers

As computers became networked online, bots known as "web crawlers" were developed to autonomously mine data[51] from the internet[52] by "fetching" (accessing) a web page[53] and "extracting" (recording) its data in a process known as "scraping."[54] The first web crawlers were programmed to report internet usage statistics, but bots known as "spiders" emerged to fetch, scrape, and index a rapidly growing body of online content,[55] eventually evolving into the first online search engines.[56]

In fact, despite the term's invasive or hostile connotation, scraping underlies much of the quality information users have come to expect from the internet: ongoing price information on sales across millions of websites,[57] weather data compiled from local stations,[58] or online statutory and case law sources facilitating free legal research.[59] Businesses use customized crawlers to scan for online mentions of their ***850** company in order to police intellectual property or discover public relations (PR) opportunities.[60] Academics use them to collate copious amounts of online data; the Google Scholar crawler, for example, indexes academic articles[61] and played no small part in this Article.

However, some web scraping is malicious; bots can collect emails, phone numbers, and other personal information exposed online (either intentionally or inadvertently) and use the data for identity theft. Scraped data like text and images can be republished, giving rise to ample criticism of its legally ambiguous practice[62] and a technological arms race between scrapers and content creators.[63]

Crawlers may meet the act's bot definition in that their behavior is mostly automated and not the result of a person. Whether they are "online account[s]" remains unclear, as the term is undefined in the act. But even if crawlers are bots under the CA Bot Act, they generally interact with web pages and other software rather than with people,[64] and most of them likely do not implicate the CA Bot Act.

b. Bots that Talk Directly to People: Chatbots

Because the CA Bot Act regulates bots that interact "with a person," a clearer case exists for "chatbots" (also known as "chatterbots,"[65] "virtual assistants,"[66] or "artificial conversational ***851** entities"[67]), which use natural language processing (NLP)[68] to imitate conversation via text or audio and respond to a user's input with appropriate-seeming responses.[69] As a chatbot might put it, they are *bots* that *chat*.

Among the earliest commercial applications of chatbots was for customer service,[70] and it seems to be their largest commercial use still today.[71] As online customer-service representatives, chatbots offer businesses many advantages over human employees: comprehending and responding to customers' inquiries more rapidly, communicating with multiple customers simultaneously, needing no downtime or labor protections, and unfailingly staying calm with impatient or irritable customers.[72]

Beyond customer service, chatbots are being developed and used to fulfill communicative professions of all types: financial advisors,[73] career counselors,[74] legal consultants,[75] poll takers,[76] assistants for ***852** dementia patients,[77] and even a return to the first chatbot's job as a therapist.[78]

Some chatbots are monitored and instructed by their developers to improve performance,[79] but chatbots mostly input, process, and reply to conversation, and it seems fair to say that substantially all of their behavior is automated. Accordingly, they likely constitute "bots" regulated by the CA Bot Act.

Moreover, their name and purpose strongly suggest that chatbots also meet the first element of a CA Bot Act violation, because they *communicate directly* with persons. As this Article demonstrates, a more nuanced analysis is needed to examine social bots, which can communicate with people indirectly.

c. Bots that Talk Indirectly to People: Social Bots

The enormous growth of social networks[80] has birthed the social bot,[81] an autonomous agent that creates an online account to complete tasks a human user does, posting content and feedback.[82] Emails, private messages, and replies to an individual's post or comment would seem to be "communicating or interacting" with a person online. But a closer question exists as to whether simply publishing online content *not directed at a particular individual*--for example, a social bot posting fake news or leaving a product review--would suffice as indirectly communicating to trick a person: Is an online bot's public posting effectively communication with every user who reads it?

***853** Relevant case law suggests the answer may be yes. A CA Bot Act violation can be brought as an act of fraudulent deceit, and California courts have held in such cases that a deception may be "indirect."[83] "Although not made directly to" a potential plaintiff, misrepresentation may be actionable if made to a third person that the defendant "intends or has reason to expect the third party "will [repeat] its substance" to others, "influenc [ing their] conduct in the ... type of transactions involved."[84]

Social networks exist specifically to facilitate communication and interaction between different accounts. Endorsement features (for example, "liking" or "retweeting") communicate opinions, deriving value from publication and affecting the content's visibility and publicly posted rating. Privacy settings notify users when their behavior or speech will be visible to other online accounts. Moreover, social media inherently facilitates republishing communication. Apart from reposting, even commenting on a post often notifies a user's linked contacts, renewing the post's visibility and effectively forwarding it.

The superhuman ability of botnets, networks of large numbers of bots, to send and respond to speech and manipulate visibility magnifies their foreseeable reach. Information is shared intimately between people across vast distances, driven largely by perceived interest, thereby expanding the list of potential recipients of a bot owner's fraudulent communication. Bots often mine and utilize user contacts like email addresses, URLs, and phone numbers, and such bot owners may be hard-pressed to deny the patent foreseeability of their reaching virtually any user on a social network, or even anyone on the internet in general.

Thus, a bot owner using social bots to tweet content that disparages a candidate in a public election might be characterized as intending to deceive and influence the votes of any voter who viewed the tweet, even one who saw only a screenshot bearing the bot's Twitter account name.

Unlike crawlers, chatbots and social bots then likely meet the CA Bot Act's first element. And as this Article shows, the foreseeability that a message will be republished also bolsters the argument that chatbots and social bots fulfill the CA Bot Act's second and third ***854** elements: *intending to mislead* people online, *by tricking them into believing* the bot is actually a human.

2. The CA Bot Act Regulates Bots that Pose as Humans

In contrast to prior bot regulation that targeted the bots' deception of *computers* by bypassing their security measures,[85] the CA Bot Act regulates *bots that deceive the human recipients* of their communication.[86] Therefore, proving a CA Bot Act violation is likely to rely less on forensic experts testifying on computer code and ticket-sale rates, and more on alleging that a bot's online traits and behavior would convince a reasonable person that the bot's speech came from a human.

Notably, many of the facts evidencing an "intent to mislead" (e.g., using a fake name) would likely also demonstrate a purpose to deceive; thus, the two elements will be examined in conjunction.

a. Chatbots

One of the first functioning chatbots imitated a psychiatrist, offering questions and responses in text form, and was highly effective at fooling people--far more than its inventor, Joseph Weizenbaum, had expected: "I was startled to see how quickly and how very deeply people conversing with [ELIZA] became emotionally involved with the computer and how unequivocally they anthropomorphized it."[87]

Indeed, communicative bots are evaluated not for their complex logical reasoning skills or the breadth of their vocabulary but rather their ability to fool human users into believing the bots are fellow humans.[88] Chatbots' utility largely derives from an ability to deceive, ***855** and many of the arguably benign or even beneficial customer-service chatbots employed on commercial websites feature images, avatars, real names, and casual language,[89] seemingly to induce belief the bot is a concerned human.

Chatbots' indefatigably sunny disposition is aimed at consoling people; research suggests humans' willing credulity[90] is driven by a desire to be heard,[91] and many online customer-service requests are made to blow off steam as much as meet a need.[92] Given their deception by design, chatbots' behavior frequently displays the requisite intent and knowledge under the CA Bot Act.

Nothing may be lost if a bot discloses itself, and even chatbots embracing authenticity might reap the benefits of using human-like language; one industry office says that in its user testing, when customers get a bot "response with an emoji, I've seen the smiles[;] people know it's not real and don't care that it wouldn't pass a Turing test."[93] Communicating by text may have coded within us a Pavlovian response, and even a *disclosing* bot's human-like conversation might comfort or charm.[94]

The hard cases could come from what might be termed "therapeutic chatbots,"[95] like the original chatbot, ELIZA, which functioned as a patient and reportedly effective AI-driven *therapist.* ***856** Chatbots can converse with abuse or war[96] victims to help them process trauma as an anonymous companion that does not "ask them questions or judge them or ... give them opinions."[97] However, in such examples the user is aware the chatbot is a bot. The ethics of an online chatbot posing as a real medical professional seem at least complicated. Doing so for money might violate the CA Bot Act.

b. Social Bots

Similarly, social bots' artificial online identities feature fake names, avatars, and images, seemingly to convince human users on the online social network (OSN) that the account is run by a real person. More sophisticated social bots act as "identity thieves," copying information (e.g., names, bio, profile information, photographs) from accounts on the OSN or scraped from the internet,[98] sometimes altering it slightly to avoid detection,[99] giving them a "veneer of humanity" in many cases by creating online accounts that organically appear to be accounts created by real people.[100]

California case law on fraud indicates that both the intent and knowledge of a communicated misrepresentation can be inferred from "false representations made recklessly and without regard for their truth in order to induce action by another."[101] Thus a bot owner's *intent to deceive* (by conveying an impression that the bot is a person) might be inferred from the account's featuring a realistic name or scraped images to bolster its authenticity. Employing "natural language ***857** programming" to respond to humans might also evidence the bot owner's plan to dupe users into believing the bot was a person.

The more realistic the bot account, the stronger an argument that all of its human-like behavior (commenting, replying, posting) constitutes evidence of an intent to mislead. Even the absence of disclosure can itself suggest that the bot user intended to deceive other users.[102] There is thus a strong case to be made that most social bots meet the second and third elements. And anyone in California who makes a purchase mistakenly relying on a deceptive bot's online review or electoral fake news might have a basis to sue under the act and attempt to unmask the bot owner.

3. The CA Bot Act Regulates Bots that Try to Influence People

Social bots act maliciously in a number of ways. They seek to increase connections ("adding friends" on a social network) by "spear phishing,"[103] then leverage the resulting trust and access in order to copy "large volumes of private data ... that are publicly inaccessible."[104] That data can then be used to bolster another social bot's apparent authenticity, send the data's owner appealing-sounding malware links,[105] or deduce correct answers to security challenges in online password-retrieval systems.

But beyond copying the personal information of human users on OSNs, social bots seek to influence the humans themselves. Traditionally, malicious programs (e.g., malware and viruses) "attack vulnerabilities of hardware and software, [whereas] social bots exploit human vulnerabilities, such as our tendencies to pay attention to what appears to be popular and to trust social contacts."[106] That is to say, *social bots cause harm by leveraging a user's belief the bot is a real person in the world*.

***858** Social bots can be programmed to express support for certain words or ideas or to verbally attack their critics, and human users of the social network may assign the bot's behavior undue attention and value, believing it represents an actual individual's thought or opinion. Such a misunderstanding can be formidable in the aggregate; large numbers of bots can be coordinated into a botnet to create a false impression of individual consensus, contaminating online data like a product's popularity or public opinion on political candidates, proposed laws, or issues of public concern.

a. The Commercial Prong

A deceptive bot might communicate in a manner violating the CA Bot Act's commercial prong in many ways, along a spectrum from soliciting a purchase, to recommending a product on a web page selling the product, to simply using bots to endorse (or denounce) a business's online presence. Provided the bot offers commercial information by posing online as an authentic human, a Californian user who reads the bot's communication arguably renders the behavior illegal under the CA Bot Act.

b. The Political Prong

With everything from coffee cups to chicken sandwiches politicized in the national dialogue, virtually any election-related media sent by a bot-- fundraising, campaign advertising, voter guides, fact sheets, and even the news--might be evidence of the original bot owner's intent to influence a vote.

There are guides a court could consider, like the timing, proximity, and reference to an election. But nowadays, the campaign never ends. And the challenge of trying to ascertain exactly what the law covers can look a lot like unconstitutional vagueness. Accordingly, the matter is taken up in Part IV.

D. Adequate Disclosure Under the CA Bot Act

Assuming a plaintiff can properly allege that a defendant-bot owner's behavior required disclosure, the plaintiff will likely have to allege and almost certainly have to prove the bot owner failed to disclose adequately under that statute. Therefore, this Article next turns to assessing the standard and fact pattern that might constitute the requisite disclosure under the CA Bot Act.

*859 1. Disclosure Must Be Proven in a UCL or Concealment Action

In order to prove a violation of the UCL's unlawful prong by "borrowing" the CA Bot Act, a plaintiff must allege that the CA Bot Act has been violated. Furthermore, in a fraudulent-deceit action, a court will need to determine what duty the CA Bot Act imposed on the defendant and whether a *material fact* was *omitted*.[107] Thus, both legal theories require an assessment of proper disclosure.

2. What Constitutes Adequate Disclosure?

On its face, the CA Bot Act permits people to use online social bots to administer and communicate with social networking accounts, provided the bot discloses "that it is a bot" in a manner that is "clear, conspicuous, and reasonably designed to inform persons with whom the bot communicates or interacts."[108] This standard involves a measure of vagueness. As the Federal Trade Commission (FTC) says, in the realm of online disclosure, clear and conspicuous is "a performance standard, not a font size."[109]

But the FTC's advice is nonetheless instructive; factors to consider include whether the disclosure is prominently placed, unavoidable, obscured by competing information, repeated, and understandable.[110] The need to scroll a web page in order to read the disclosure should be avoided, as should pop-ups; interactive pop-up chatbots should disclose they are bots when they first greet a customer.[111] The CA Bot Act's legislative history suggests the use of distinguishing text and color.

One thing to consider would be a fairly clear California case law principle sometimes called the "click-wrap" or "browse-wrap" rule: a user's consent to an implied online contract is more likely if users must *860 click acknowledgement of the online notification.[112] Merely providing a link to language for the user to browse is often insufficient to bind the user.[113] The rule recognizes the indirect manner in which a user may arrive on a website and the ability of a user to use the website without ever seeing the pages containing the contractual language or warning.[114] Requiring a user to affirmatively acknowledge a bot's disclosure before communicating is therefore more likely to meet the CA Bot Act's disclosure rules than merely providing notice a recipient user must seek out.

Next to consider are causation and harm. Those elements are far more speculative without a real-world example to analyze, but both of California's potential enforcement vehicles--the California Unfair Competition Law and the tort of fraudulent deceit--offer a number of helpful inferences and guidelines to assess both "reliance on" misleading speech and consequential "harm." They are discussed in Part III.

III. Suing to Sanction a CA Bot Act Violation

A. Enforcing the CA Bot Act Requires Showing Causation and Harm

The CA Bot Act provides a legal standard for illegal behavior; it does not redress any of the effects of that behavior. A human user receiving the bot's communication need not believe the bot is a person in order to prove a violation. Government attorneys can likely prosecute ***861** bot users without the need to prove harm to any particular individual. But sanctioning a bot owner with a *private* civil action under California's Unfair Competition Law,[115] the state's fraudulent-deceit statute,[116] or any fraud theory[117] inherently requires alleging and proving reliance on the misrepresentation and a resulting injury. Thus, this Part examines the elements of causation and harm[118] for standing and substantive purposes.

B. Two Legal Frameworks for Sanctioning CA Bot Act Violations

Despite its lack of an articulated enforcement provision, the CA Bot Act can likely be enforced via civil actions under California's Unfair Competition Law and tort of fraudulent deceit. Both legal mechanisms can reach deceptive behavior that violates other statutes, and proving a CA Bot Act violation would be sanctionable under either. The UCL's penalties are expressly "cumulative" of any other penalties,[119] and an action could plead both theories, at least for sanctioning violations of the commercial prong since the UCL applies only to commercial fraud.

1. California's Unfair Competition Law

a. The UCL Permits "Borrowing" Laws to Define "Unlawful" Business Practices

The UCL prohibits "unfair competition,"[120] defined as *"any unlawful*, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising."[121] Plaintiffs may "borrow" violations of other laws to stand as unlawful practices "independently actionable" under the UCL, provided the borrowed statutes are "pursuant to business activity."[122] Such actions are independent from those under the borrowed statute; the UCL offers "distinct ... equitable remedies for unlawful business practices," and other laws define only ***862** what is unlawful.[123] Thus, even if a commerce statute fails to create its own civil cause of action,[124] a plaintiff can effectively enforce it with a suit to enjoin or sanction the unlawful behavior under the UCL's so-called unlawful prong.[125]

There are limitations to the doctrine; a UCL action cannot borrow the violation of a statute that explicitly prohibits a cause of action,[126] nor can it proceed if it is *federally preempted*.[127] State statutes may generally be preempted by federal law when they (i) "encroach on a field fully occupied by federal law," or (ii) "stand as an obstacle to the accomplishment of the federal objective."[128]

b. The UCL's Borrowing Doctrine and the CA Bot Act

The CA BOT Act's commercial prong explicitly addresses misrepresentation in commercial transactions. The act does not bar a private action, and its duties are cumulative with "any other duties or obligation."[129] Furthermore, no current federal law governs bots posing as humans to incentivize commercial transactions with people.[130] The federal Better Online Ticket Sales (BOTS) Act (prohibiting "scalper bots") may regulate bots posing as humans,[131] but it governs a bot's engagement with other computers (circumventing their security measures) rather than attempting to mislead human users.[132] And if ***863** anything, the CA Bot Act reinforces the BOTS Act's goals of honesty and clarity as to whether online actors are real people.[133] Given its

commercial and cumulative nature, as well as a lack of relevant federal preemption, the BOTS Act can likely be "borrowed" for a civil action under the UCL.

2. Fraudulent Deceit

a. Violations of Disclosure Statutes Can Constitute Fraudulent Concealment

California's statutory tort of fraudulent deceit is similar to intentional fraud[134] but addresses harmful deceptions that are not contract based. The statute prohibits "willfully deceiv[ing] another with intent to induce him to alter his position to his injury or risk."[135] One of four defined types of deceit is concealment: "The suppression of a fact, by one who is bound to disclose it, or who gives information of other facts which are likely to mislead for want of communication of that fact."[136]

California case law provides four ways a duty to disclose may arise (i) by statute, (ii) by contract, (iii) through a fiduciary relationship, or (iv) "as a result of other conduct by the defendant" making it "wrongful ... to remain silent."[137] The CA Bot Act expressly provides a duty to reveal that a bot is not a person. Thus, violating the CA Bot Act constitutes an intentional omission of a duty to disclose a material fact and should be actionable concealment under fraudulent-deceit law.

b. Violations of the CA Bot Act's Political Prong Can Be Concealment

Many overlapping issues are raised by UCL and fraudulent-deceit claims, but important distinctions exist. For example, while the UCL prohibits imposing punitive damages, they are ***864** recoverable for concealment.[138] Most importantly, unlike the UCL, fraudulent deceit is not limited to *commercial* misrepresentations,[139] and even violations of the CA Bot Act's political prong (fraudulent bot use to influence a vote) might very well constitute actionable concealment under fraudulent deceit.

Thus, civil actions can sanction a CA Bot Act violation. Accordingly, the next Section explores potential plaintiffs and defendants in such actions and considers how to articulate causation and harm.

C. Public Prosecution for CA Bot Act Violations via the UCL

1. Standing to Sue in California

Generally speaking, plaintiffs have standing to sue only when they demonstrate (i) an injury in fact (ii) was caused by the circumstances or behavior in question (iii) that can be redressed by the lawsuit.[140] This inquiry is generally designed to ensure that courts hear only actual controversies.[141]

Standing in California can also be conferred by statute.[142] For example, the UCL authorizes *public attorneys* to sue violators for civil penalties (up to $2,500 per violation) or injunctive relief,[143] including under the borrowing doctrine.[144] Such actions offer a particularly ***865** appealing path for prosecuting a CA Bot Act violation. While private actions require a showing of causation and harm to the plaintiff, the UCL is a strict-liability statute,[145] and a public prosecutor bringing an action under the UCL need not show the plaintiff's injury, neither for standing nor to seek civil penalties for a violation.

2. Compelling Government Action to Enforce the UCL Against CA Bot Act Violators

Notably, the California Constitution contains no "case or controversy" provision expressly limiting judicial review, and standing *has been found* in California without needing to prove the kind of concrete and particularized injury necessary for federal review.[146] Under a "public right-public duty exception" to the rule that a petition for mandate must be brought by a beneficially

interested party,[147] a California resident or entity might even have standing to seek a writ ordering the state attorney general to enforce the CA Bot Act against violators engaged in unfair competition.[148]

Interpreting a statute's language to determine its boundaries of standing relies to a large extent on legislative intent,[149] and the California citizenry's express removal of the UCL's option to sue in the public interest flies in the face of self-interested white knighting.[150] A public-interest basis for standing has limits,[151] further abated by more recent rulings in California courts.[152] But the same courts have noted the UCL's "legislat[ive] intent to discourage business practices that ***866** confer unfair advantages in the marketplace to the detriment of both consumers and law-abiding competitors."[153]

Such an action might offer little immediate pecuniary incentive to a potential plaintiff, but a consumer group, like the CA Bot Act's sponsor,[154] might seek standing to force the government's hand. Moreover, the California Supreme Court has held that the UCL's reference to a business practice indicates that "the statute is directed at *ongoing* wrongful conduct,"[155] and so "a pattern of behavior" or "course of conduct" can be treated as multiple violations warranting additional penalties.[156] Even under more restrained calculation formulas, public UCL actions to sanction *ongoing online misrepresentation* have extracted substantial sums from violators.[157] Given the ability to magnify damages,[158] and no need to show harm, public prosecutor actions in California to sanction CA Bot Act violations might prove an effective tool to unmask perpetrators and police malicious social bots in the commercial sphere.[159]

D. Reliance on the Mistaken Belief that a Bot Is a Person

The UCL also authorizes *private* "actions for relief,"[160] although the UCL's prior standing language was broader.[161] In 2004, private ***867** actions in the public interest were cut from the UCL, narrowing the class of private plaintiffs with standing to people or entities who have (i) suffered injury in fact and an actual loss of "money or property," (ii) "as a result of" the violation of a borrowed law or other unfair competition.[162] Assessing these standing requirements overlaps with California courts' analysis of causation and harm under the UCL,[163] and the various issues are treated in conjunction.

1. Reliance Under the UCL

a. Purchasers Relying on a Product's Mislabeling Have Standing Under the UCL

In private actions under the UCL, causation is a separate element requiring proof.[164] The UCL causation standard ("by means of") is "less stringent than but-for causation,"[165] but plaintiffs fail to show causation if they would have "suffered the same harm *whether or not"* the law was violated.[166]

The threshold is still arguably low, as first defined in *Kwikset Corp. v. Superior Court*,[167] which states that consumers who were honestly "deceived by a product's label into spending money to purchase the product, and would not have purchased it otherwise, have 'lost money or property"' under the UCL's standing provision, even if the purchase was in no way "overpriced or defective."[168]

In 2013, the US Court of Appeals for the Ninth Circuit interpreted *Kwikset* to reject a defendant's argument that there was no injury in mislabeling if a product itself was inherently the same and ***868** had not changed in quality.[169] A plaintiff "who relies on a product label" containing a misrepresentation can satisfy standing for a UCL action if the plaintiff "would not have bought the product but for the misrepresentation."[170]

As a California appellate court noted approvingly in mid-2018, under *Kwikset* the UCL's injury-in-fact standard has been interpreted rather broadly, reflecting a kind of subjective reliance on the plaintiff's good-faith allegation of having made a purchase but for the misleading claim.[171]

b. Online Bots Seek to Induce Commercial Transactions by Posing as People

Social bots act as what computer scientists call "sybils" or "sockpuppets,"[172] false identities "created to ... increase the power or resources of a single user."[173] For example, they can pose as objective individuals and indicate their support[174] for a person, product, company,[175] or even an idea, often in a coordinated effort en masse, thereby artificially increasing the bots' visibility and credibility.

***869** In "social commerce,"[176] social bots pose as real purchasers[177] and sellers to influence real users by authoring and posting reviews of products or services on business sites or "collaborative content rating, recommendation, and delivery systems" like Twitter[178] and Facebook.[179] Even online commerce juggernaut Amazon admits that its most advanced algorithms can't stop all such autonomous activity,[180] including bot-composed reviews more believable than real ones.[181] The barriers continue to drop, as social bots are "sold in bulk by the thousands" to merchants,[182] and software available online allows inexperienced users to set up and administer multiple social-network accounts with bots.[183]

The pernicious effects of a false endorsement or criticism become magnified on the internet through a process known as information cascading, wherein internet users tend to trust large-scale consensus ***870** over their own opinion or independent research, triggering a chain reaction of "herd mentality"--driven behavior.[184] This phenomenon is amplified by coordinating a series of accounts to collectively praise (or denounce) a particular point of view to cause information cascades. Known as "crowd-turfing,"[185] such paid endorsement can be starkly effective. When thousands of online accounts suddenly focus on a subject, they can drive attention to it by synchronizing their hash-tags, causing trending algorithms to give prominence to the bot owner's viewpoint. Hashtags can also be tagged deceptively, drawing interested users to confront them with unrelated and controversial content.[186]

At the commercial level, businesses conduct these campaigns either to pose as approving consumers or, perhaps more insidiously, to "fabricat[e] nonexistent accounts of bad experiences or service" by a competitor.[187] The problem is exacerbated by the growing influence of online reviews, and the FTC has observed the consumer harm in such information being misleading; the agency requires celebrities and "influencers"[188] to disclose if they are being paid for their endorsements.[189]

871** ***c. Online Users Could Show Injury Was as a Result of Deceptive Bot Speech

Given the preponderance of misleading social bots online, some plaintiffs will likely be able to allege enough harm to bring actions under the UCL by claiming reliance on a defendant-bot user's communication in purchasing and "borrowing" the defendant's violations of the CA Bot Act.

A plaintiff hoping to show causation of harm by an illegal social bot would allege not only reliance on the bot's communication (e.g., that he only bought this product because of the positive review) but on the mistaken belief that a real person had authored it (e.g., if he had known it was not a person, he would have ignored that review, or the product's overall rating, and would not have bought the product).

A complaint might point to similar facts supporting the intent element: the bot's use of images and content, as well as its natural language programming and ability to communicate using human-like expression, gave the impression it was an account administered by a real person.

Specificity in the pleading is paramount--naming emails or other ways the misleading content was communicated, with specific dates,[190] as well as alleging with particularity how the bot was deceptive (e.g., false name and avatar or conversational tone) and asserting that it was done with the intent to defraud. With the anonymous nature of online speech and a judicial standard for reliance that defers in part to plaintiffs' good-faith credulity and personal reasons for making a purchase, consumer-plaintiffs likely would have a wide array of details and facts to marshal and have a colorable chance at proving they mistakenly believed the words of a deceptive online social bot were that of an actual person.[191]

2. Reliance Under the Law of Fraudulent Deceit

Much of the reliance element's analysis applies equally to either statute. People harmed as a result of believing that the bot communicating with them was a fellow person will often be able to claim "justifiable reliance," as required in a tort action for statutory deceit. ***872** Nonetheless, analyses in deceit actions offer a number of principles worth considering in applying concealment to bot activity.

a. Misrepresentation Need Only Enter into the Decision-Making

Case law in actions for deceit indicates that a plaintiff's reliance on a misrepresentation must be a substantial factor in the alleged harm but "need not be the sole cause of the damage."[192] Thus, the attraction of an online vendor's same-day delivery need not displace the materiality of the vendor's online rating in a purchasing decision, and if the rating were artificially boosted by bots, the buyer could rightly claim reliance on the bot owner's omission of a statutorily mandated disclosure.

Indeed, the informational feedback afforded by social commerce is unprecedented, and the ability to view and consider an enormous number of representations about a product (popularity, user experience, quality comparison) makes explicit that decision-making involves many factors. Acting on their purported accuracy may effectively mean being duped by deceptive bots' misrepresentations.

With the majority of internet traffic occupied by bots, and 20 to 30 percent malicious bots,[193] one is left to wonder how much online product info is authentic and how much is BS (bot speech).

b. Plaintiffs Are Not Expected to Guess Who Is a Bot

In considering whether reliance was reasonable, a plaintiff's negligence "in failing to discover the falsity of a statement is no defense when the misrepresentation was intentional."[194] Fact-finders should "take into consideration plaintiff's intelligence, knowledge, education and experience,"[195] and people are not held to a standard of elevated precaution or minimum knowledge.[196]

***873** Although most people in the United States are now active on social media,[197] their sophistication with respect to technology and social media conventions may range in geography, age, and education. Under general principles of fraud, a less tech-savvy boomer plaintiff might not be expected to realize that a social media account is a bot just because an experienced millennial Instagram influencer would know.[198]

c. Reliance Should Be Clearly Articulated in Detail

Under California law, proving intentional fraud demands a higher standard of pleading, requiring specific allegations by the plaintiff of "who said what to whom and when and where."[199] Accordingly, every element of violative bot behavior and how it incentivized a commercial transaction or influenced an electoral vote should be articulated in the initial complaint--which should also include articulations of specific electronic records with dates and even time stamps, corroborating evidence, and the forensic information technology skills (or expert testimony) to articulate what records can be requested--in discovery in order to demonstrate how a particular defendant is at fault. A similar specificity should apply to subpoenas of John Doe ("Doe") defendants, as is explored more extensively in Part IV.

E. How Does a CA Bot Act Violation Cause Harm?

Pecuniary injuries are generally more articulable and demonstrable than nonpecuniary ones and are thus more easily recovered.[200] A plaintiffs' class in a UCL action based on a CA Bot Act violation might consist of online purchasers of an air conditioner, relying on a belief that a large number of positive reviews represented the communications of actual human purchasers, rather than social bots. Each proven purchaser who relied on the high rating might recover the purchase price in penalties.

By contrast, noneconomic harm, such as emotional distress, can be harder to allege and prove, and an injury caused by having one's vote influenced in a misleading manner seems harder to imagine and ***874** articulate. Neither law nor equity remedy *butthurt*.[201] That said, well-documented uses of deceptive bots to target and harass online users, or to attempt interference in political elections, offer real-world examples that might give rise to actions for violating bots' noneconomic harm.

Given the more salient harm and clearer fact pattern in actions for economic injuries, this Section examines such injuries first, before turning its attention to the thornier task of noneconomic harms.

1. Economic Harm

a. Harm Under the UCL

The UCL redresses only injuries to money or property[202] and even excludes recovery under certain traditional theories of economic harm, like disgorgement.[203] Nonetheless, the UCL's injury standard under *Kwikset*[204] suggests that if a consumer's purchase is made on the basis of an intentional misrepresentation, *the purchase itself* constitutes a harm, regardless of the product's or service's quality.

A consumer's taste and criteria need not be reasonable--only honestly alleged; indeed, *Kwikset* itself granted relief to a patriotic plaintiff who believed a false claim that the locks he bought were "made in America," despite a district court finding the locks suffered no loss in quality.[205]

Moreover, *Kwikset* has frequently been broadly applied; amid a line of cases sanctioning falsely claimed price reductions, a California appellate court referenced the UCL's consumer-protection purposes, stating that the "phrase [injury in fact] ... is not synonymous with 'actual damages,' which generally refers to pecuniary damages. Rather, the consumer must merely 'experience some kind of damage,' or 'some type of increased costs' as a result of the unlawful practice."[206]

***875** If phony price drops have earned multimillion-dollar civil penalties in UCL actions,[207] one can imagine that employing networks of automated online accounts to pose as consumers and deceptively review products and services could meet the same standard. Harm might only be the purchase price, though under the UCL the ongoing presence of fake reviews could warrant

multiple penalties--far more in class actions, which are frequently used under the UCL.[208] And while the burdens of class-action standing[209] and certification[210] prevent obstacles, vendors *have* been caught posting fake reviews under fictitious names to remedy or raise their online profiles.[211] If the social network amplification industry's advance[212] receives enough ***876** publicity[213] to grow a sense of urgency, class actions with the ability to multiply civil penalties for ongoing online behavior might incentivize a rise to the challenge.

A commercial vendor-plaintiff that can specifically allege and provide evidence that a competitor is using deceptive bots to write positive or negative reviews, or artificially increase the competitor's rating or visibility, might also be able to sue under the UCL to enjoin the bot behavior and seek to unmask the violators with a preemptive subpoena on the ISP or network hosting the content.

The CA Bot Act only prohibits a deceptive practice in commerce; a competitor harmed by its violation need not be the person with whom the deceptive bot communicated. Online review scores bestow prominence, visibility, and endorsement on websites[214] and have even been monetized,[215] and *amplifying* them *with bots posing as real reviewers* arguably injures competitors in the marketplace (particularly on the same commerce website) as a result of an illegal deceptive business practice.

The UCL does "not require the courts to protect small businesses from" legitimate competition, and the California Supreme Court has said that "unfairness" in a competitor claim under the UCL must derive from legislative intent.[216] But vendors using deceptive bots to mislead consumers, or game the system by manipulating online searches with artificial data, distort the competitive process in precisely the "unfair" manner that the UCL is aimed at preventing.[217] Indeed, the UCL is designed to "[sweep] within its scope acts and practices not specifically proscribed by any other law," anticipating any unnamed or unforeseen ***877** "new schemes" being "contrived" by "human ingenuity and chicanery."[218]

The planning and the doing are different matters, however, and any such action likely involves a significant logistical and factual challenge of showing that the comments are fake, bots were used, and the product's seller is responsible for the activity. And better-designed bots continue to outwit technological efforts to detect and repel bots. Vendors' online forums regularly feature laments of having to compete with sellers purportedly using social-bot reviews to gain visibility.[219] The cheapest bots are often brand-new online accounts started within days of each other, giving five-star ratings with terse, vague, and low-effort endorsements that often suspiciously use overlapping verbiage and praise.

But many organizations, security firms, and online sites offer software and techniques to identify likely bot accounts by analyzing metrics like the timing, frequency, and content of a social media account's activities and posts. Under certain case law, a competitor might even be able to claim the cost of investigating and identifying the defendant's unfair conduct as the injury, though other rulings may cast doubt.[220] In any event, online vendors faced with narrow margins and deceptive competitors might possibly be organized, combining their resources to root out the practice.

b. Harm Under Fraudulent Deceit

To prove fraudulent deceit, plaintiffs must show they were injured by a change in position made in reliance on the misrepresentation. Altering one's position can include entering into a contract in reliance on a misrepresentation,[221] as well as related costs, ***878** like quitting one's job and moving across the country in reliance on misrepresentations about employment.[222] Thus, many of the contemplated actions for economic harm under the UCL could be brought under concealment or another deceit, with the added benefit of a wider range of remedies, including punitive damages.

2. Noneconomic Harm

a. Physical Pain, Mental Suffering, and Emotional Distress

No fixed or absolute standard exists in California to compute the monetary value of noneconomic damages like "physical pain, mental suffering, and emotional distress,"[223] and a fact-finder is "entrusted with vast discretion in determining the amount of damages to be awarded."[224]

In light of the internet's knack for propagating misinformation,[225] the relatively broad concept of detrimentally altering one's position in reliance on data offered by a deceptive bot unmasks an almost tantalizing array of possible scenarios for alleging deceit via the CA Bot Act.

Bots post fake news to misinform voters and stir the pot in political discussion. For example, in the debate over mandatory vaccination and its claimed health risks, Russian bots post misleading health information online "to create impressions of false equivalence or consensus," clouding available information and increasing confusion and contentiousness over the issue.[226]

Could the CA Bot Act help compensate parents whose child became ill after they refrained from vaccinating a child or other medical intervention by relying on a deceptive social bot's online health claims?[227] What if the bot was posing as a fellow parent or health professional and the health claims were directed at relevant parties, ***879** like online users announcing their recent birth on social media or members of a Facebook group for new parents? What if a botnet were used to give prominence and visibility to a claim or an organization's viewpoint?

Notably, the deceit law redresses plaintiffs' acting in reliance "to [their] injury *or risk*," though in this Author's research the term "risk" is only used when the statute is quoted, and its meaning remains unexplored. Thus, a more speculative harm might be sanctionable, particularly if specifically articulated and bolstered by credible expert testimony.[228] Recovering for speculative personal injury caused by a concealment is hardly without precedent,[229] including massive class certification for plaintiffs exposed to a campaign of deceptive behavior.[230] A well-articulated pleading might at least advance the action to discovery, where more information about the bot's origin can be deciphered.

Malicious bot activity, including efforts to influence online political discussion, has been reported since they first appeared online in Internet Relay Chat (IRC), an early chat-room application.[231] IRC moderators described "antisocial behavior" as "not rare" and "[r]acist and homophobic outbreaks" as "regular events," sometimes with the use of bots to flood channels with negative messaging.[232] One IRC veteran observes that anonymity "lowers inhibitions enough to promote self-disclosure among groups of people," often to mutually beneficial effect, but it also prompts others "to disrupt those groups and sometimes tear the delicate fabric of trust that has been carefully woven over months of conversation among disembodied strangers."[233]

***880** In fact, while some bots skew to one side of an argument,[234] bot activism is often designed to engender conflict and hostility rather than push a viewpoint; botnets posted comments in both Arabic and English on online political discussions of the Syrian War,[235] and "Russian-affiliated" social bots have been detected promoting content on *multiple sides* of controversial issues, including race relations and gun control.[236] The US Select Committee on Intelligence reported that bot accounts sit at "the far left and far right extremes of the American political spectrum," posting messages at twenty-five to thirty times the average posted by "genuine political accounts across the mainstream."[237] Other studies suggest that repeated exposure to extreme political content posted by social bots results in an exaggeration of polarization by users on both sides of the political spectrum.[238] As a researcher lamented in the Senate report, "the extremes are screaming while the majority whispers."[239]

With the national debate over the responsibility of online social networks to police fake news stymied by their immunity from ***881** liability,[240] the "sheer volume of information,"[241] claims of bias,[242] the limits of AI,[243] and a decidedly grey area as to

what can be deemed accurate news,[244] perhaps the best way to involve ISPs and social networks in the enforcement process is via subpoena. Judicial discovery might unearth some of the many unknowns surrounding the internet's many malicious bots.

*882 *b. Harm to a Plaintiff's Right to Vote in an Election*

Both the language of the CA Bot Act's political prong[245] and its legislative history[246] voice the authors' intent to prevent deceptive social bots undermining the integrity of elections. The act's record includes findings by the US Senate and Department of Justice that "Russian Government agencies, state-funded media ... and paid social media users or 'trolls"' engage in bot misinformation campaigns with "a significant escalation in directness, level of activity, and scope of effort compared to previous operations" in a "long standing desire to undermine the U.S.-led liberal democratic order."[247]

In light of this express concern, the more intriguing application of the fraudulent-deceit tort to CA Bot Act violations might be an ability to empower and redress wrongs under the act's political prong--namely, deceptive bot speech aimed at influencing a vote in an election.

Electoral and voting laws seem to offer little insight into articulating a harm element for unlawfully obstructing one's right to vote with a CA Bot Act violation. Voter suppression typically involves state action or a violation of the Voting Rights Act. Federal statutes govern constitutional torts, like witness intimidation and voting coercion, including by private actors.[248] But even if voting on the basis of misleading bot speech were deemed sufficient harm on which to base an action for, say, intimidation in voting,[249] the statute ultimately seems at best to overlap behavior prohibited by the CA Bot Act, rather than to derive its legal elements from the law as do the UCL and concealment tort.

Election-disclosure laws in California relate to fundraising data,[250] not the source or character of political speech, and the California Political Cyberfraud Abatement Act (PCAA) is aimed at "cyber-squatting" (registering a domain with someone else's name and ***883** misleading users into believing the named person is offering the content). To date, it appears no one has been prosecuted under the law.

There are constitutional torts for the deprivation of civil rights, including cases where voters were intentionally denied their right to vote, and while the US Supreme Court acknowledged it is difficult to put a number on "non-monetary harm that cannot easily be quantified," it has indicated that the Constitution might "allow the recovery of presumed general damages for certain intangible injuries caused by violations of constitutional rights," explicitly having reserved that possibility in the case of an individual's right to vote being denied.[251] However, the Court has also stated it "will not recognize presumed general damages for abstract deprivations of constitutional rights."[252]

Having voted on the basis of a misrepresentation seems a fairly abstract injury, particularly if merely the speaker's identity was deceptive, while the content communicated was accurate or an opinion. Deliberate lies in politics seem to be protected by the Constitution.[253] Obstructing the right to vote seems a more salient harm. It is unclear whether a civil action to sanction the obstruction of a vote would survive mootness or redressability inquiries, let alone be compensable (nominally or otherwise), but sufficiently egregious behavior could conceivably warrant judicial liability. Regrettably, potential actions are best illustrated by real-world reports of efforts to mislead voters into missing their vote.

In the past fifteen years, (i) Latino US citizens registered to vote received mailings (incorrectly) warning them, in Spanish, that voting in a federal election as an immigrant could result in prison time; (ii) fliers were distributed in largely African American neighborhoods falsely warning that people with outstanding warrants or unpaid parking tickets could be arrested if they showed up at the polls on Election Day; (iii) students received fliers stating that in order to vote in a local precinct, they had to pay to change their driver's license and reregister vehicles in the city in which the precinct was located; (iv) people reported receiving

text messages on Election Day telling ***884** them to wait to vote until the next day; and (v) others received calls falsely informing them that they could vote via telephone.[254]

The dangers are real, and using social bots to discourage individuals from voting is hardly science fiction.[255] Twitter took down a 10,000-account botnet doing precisely that.[256] Bot campaigns to mislead voters into going to the polls the wrong day, or intimidate them into not voting, might violate the CA Bot Act's political prong by attempting to influence an election vote. The violation would offer per se evidence of fraudulent deceit and could conceivably support an injunction to remove offending accounts and subpoenas to unmask the bot owners. Thus, the CA Bot Act could be not only a means of compensatory justice but also a tool of removing deceptive information from political elections.

3. Remedies

a. Remedies at Law

The UCL authorizes courts to make orders "necessary to restore to any person in interest any money or property, real or personal."[257] Civil penalties are limited to the plaintiff's injury but could be substantially compounded by a class action or for ongoing behavior. It is also worth mentioning that a CA Bot Act violation might also violate California's Consumer Legal Remedies Act (the "Lemon Law"). UCL and Lemon Law violations are often alleged in a single action,[258] and ***885** the latter's doubling of civil penalties can offer substantial additional financial incentive to a UCL class action.[259] That said, neither statute allows awarding punitive damages for a violation, however egregious.

By contrast, a concealment tort can justify punitive damages, and while deceit is sometimes construed as a breach--constraining an award to contractual damages[260]--exemplary damages have been awarded in fraud actions for shocking misrepresentations or severe noneconomic harm.

Online anonymity permits and inspires intentionally deceptive and even harassing behavior; bots are also used to assail users voicing a certain viewpoint with hostile comments and private messages.[261] Bots have been deployed to scrape or phish data used to target, "dox,"[262] and "swat"[263] individuals and groups. California's punitive damages[264] standard may very well be met.

b. Equitable Remedies

The UCL also permits public attorneys and private actors to enjoin unfair competition (behavior violating the UCL or a borrowed law), and a motivated plaintiff could possibly get a temporary ***886** restraining order on allegedly deceptive social media accounts posting bad reviews.

Perhaps most intriguing, with government intelligence predictions that online election interference will ramp up to unprecedented levels in upcoming political elections, political parties, candidates, and advocates might seek to enjoin purported deceptive social bot accounts posting election information. A political candidate might present the most salient harm but may also be tempered by First Amendment protections requiring malice for misrepresentations about public figures and matters of public interest. But if such a case could at least establish standing against a Doe defendant, a motion for preemptive discovery might help reveal the responsible parties before the election takes place. Thus, the final Part considers subpoenas to unmask Doe defendants and the often substantial constitutional safeguards preventing subpoenas from being ordered.

IV. Unmasking Anonymous Online Speech

Despite a subjective sense that users are anonymous on the internet, in many cases[265] an online posting can be traced to its author, particularly with the cooperation of the entity specifically hosting or facilitating the content.[266] Moreover, every web page a user loads "can potentially trigger dozens of nearly simultaneous web connections to various third party service providers"; no wonder that forensic computer experts collate data from a variety of sources to trace and identify online users.[267]

A. Subpoenaing ISPs and Online Social Networks' Immunity

Under the CA Bot Act's express exemption of any duty, large online publishers might have a defense to any subpoena served in violation of the CA Bot Act. However, this broad exemption does not seem to apply to smaller social networks with bot accounts or content. For example, the purveyor of a niche online dating app might be liable for failing to remove a bot account that phished private data from a ***887** human user if the app purveyor had been given prior notice of the suspected account.[268]

In any event, while section 230 provides extremely broad protection from liability for ISPs and online publishers, especially in California,[269] it does not exempt them from subpoenas to produce electronically stored info (ESI) identifying online speakers, and many have had to produce ESI.

And yet anonymous defendants have filed successful motions to quash a subpoena through the assistance of counsel and have preserved their anonymity.[270] Moreover, in California online publishers can vicariously assert an online speaker's right to speak anonymously by moving to quash the subpoena, and they too have prevailed.[271] It is therefore worth considering how such an anonymous defendant might argue for First Amendment anonymous speech protection or how one may argue to strike down the CA Bot Act.

B. The CA Bot Act Would Likely Survive Judicial Review Under the First Amendment

A number of constitutional concerns have been raised by the idea of sanctioning speech made with innovations as foreign and transient as AI, automation, NLP, and bots.[272] Indeed, an anonymous defendant might theoretically assert real First Amendment protections against the CA Bot Act's prosecution. Notwithstanding, there is substantial reason to believe the CA Bot Act is constitutional.

***888 1. Constitutional Analysis of the Commercial Prong**

First Amendment concerns are more subdued for commercial speech than political speech.[273] Likely mindful of this, the CA Bot Act's authors included a severance provision, providing that if any part of the law is struck down, the other parts can survive and continue to apply in full effect.[274]

Under either rational basis review or intermediate scrutiny,[275] commercial speech is afforded little to no protection when deemed to be misleading. Violations of the CA Bot Act's commercial prong are not only misleading but willfully so. The state can assert its qualifying interest in ensuring the accuracy of commercial information to consumers, well established by the legislative history.[276]

Disclosure is a more "benign and narrowly tailored" form of regulating speech, seen as adding information to a conversation, and if accurate and not excluding other speech, described by the US Supreme Court as sometimes enhancing the virtues of free speech.[277] The CA Bot Act requires only that "factual, uncontroversial information" be disclosed.[278] Online account owners author their public profiles, and the minor effort could hardly be described as "unjustified or unduly burdensome."[279]

Thus, the CA Bot Act's minimal disclosure and documented compelling interest suggest its commercial prong will survive. But the act's political prong poses a more involved question.

***889 2. Constitutional Analysis of the Political Prong**

The constitutional right to engage in political activity anonymously derives from association and speech freedoms.[280] Thomas Paine's anonymous pamphlet, *Common Sense*, daringly urged independence be declared, and *The Federalist Papers* were published under the pseudonym "Publius." Anonymity can increase speech by preventing reprisal[281] and improve it by reducing ad hominem arguments and focusing discourse on the speech's content.[282]

But the speaker's alleged right to pose online as another individual seems harder to defend in a context as dire as an election--which not only goes to the core of representative government and individual liberty but offers significant opportunity for irreparable harm when communication moves at a blistering pace and an election theoretically takes place only in a short, finite time period.

Indeed, protecting elections has justified even the removal of all anonymity in political speech, whereas the CA Bot Act only requires bots to disclose that they are not in fact a human, with no other condition modifying or otherwise characterizing the speech, much less identifying the speaker.

Furthermore, no other admissions, oaths, endorsements, or limits on the bot's communication are imposed, so no reprisal or chilling of speech is implicated by revealing a bot's status. At worst, a bot owner is forced to acknowledge violating most social networks' terms of service.

The political prong's soft underbelly is arguably vagueness, which is of particular concern in a First Amendment context.[283] "Vagueness" describes insufficiently predictable liability,[284] and is often paired with "overbreadth," a lack of precision such that a law reaches beyond its purported focus.

As a policy matter, one could consider which bot speech is most harmful to the election process to target potential defendants. But the ***890** CA Bot Act's "influenc[ing] an election" language might permit a truck to drive through and suffer from overinclusion. At the very least, it seems fair to say that the commercial prong is more precisely drafted than the political prong, casting less of a wide net.

Thus, absent a clearer standard, bot owner-speakers might colorably argue the law offered insufficient warning, decrying actions as "CyberSLAPP" lawsuits,[285] brought only to prod speakers into self-censorship by making them defend their online anonymity with expensive litigation.[286]

Notwithstanding, the risks of any such vagueness are obviated by the statute's inclusion of an intent to deceive by communicating with the bot. For example, a political organization using automated software to canvass or email possible voters can simply include notice of an automailer. Individuals can legally automate their speech, speak anonymously, or even pose behind a fictional persona, provided they make clear an automated software app--that is, a bot--is behaving, replying, and posting.

Thus, the CA Bot Act's reach is significantly restricted and sharply tailored to its compelling, outsized, and well-documented state interest in protecting its accurate, fair, and honest elections.

C. Enforcement of a Doe Subpoena in California

Pretrial discovery is analogous to a warrant for probable cause, raising all the skepticism of police power implied by the Fourth Amendment.[287] The dangers of forcing people to reveal their identity before even assessing the merits of an unmeritorious case on speech alone demands all the particular details and corroborating evidence expected when obtaining the right to enter someone's home. But there is an inherent tension between the plaintiff's justified attempt to proceed with an action and the defendant's constitutional right to speak anonymously.[288] California case rulings on subpoenas to unmask Doe defendants reflect an attempt to balance those interests,[289] emphasizing ***891** the needs for a strong initial evidentiary showing[290] and proper notice to the purported defendant.[291]

The political speaker's right to mislead in order to influence another's election vote seems at best *de minimis*, at worst the precise type of injury to electoral integrity that the Supreme Court has seen as a valid basis for curtailing the right to anonymous speech.[292] Political parody accounts might present hard cases, but they more likely don't violate the CA Bot Act since their satire is based around an understanding that the accounts are not operated by authentic individuals.

Some third-party publishers may resist subpoenas to preserve customers' anonymity. Employment website *Glassdoor* argued anonymity is essential to offering accurate employer reviews by employees and refused a district court order to identify users who criticized their former employer, ultimately prevailing in having the subpoena quashed at the appellate level.[293] But while such a robust defense can garner goodwill from customers, such lawsuits can generate legal fees and bad publicity, sometimes in vain. In an unrelated case, *Glassdoor* was ordered to identify eight anonymous online commenters in connection with a grand-jury investigation into alleged employment-law violations.[294]

At any rate, businesses will have to do a cost-benefit analysis of their reputation and the effort needed to mount a resistance against a subpoena rather than simply complying. And while defending employees against reprisal from former employers may engender commendable goodwill, the same may not be true of defending patently deceptive behavior intended to harm unwitting humans. It calls into question the internet's entire accuracy, safety, and reliability. Doubts cloud companies' claimed efforts to remove fake accounts when they are incentivized to claim the greatest number of users and social reach. If bots became a liability, companies might decide to more aggressively root them out.[295]

***892** Actions for CA Bot Act violations might help shift the cost-benefit calculation driving any alleged laissez-faire approaches to bots' ongoing mischief by social networks, to the extent they exist.

V. Conclusion

In a *New York Times* exposé on the professional use of social bots to boost the social network profiles of celebrities, those who benefitted from the fake accounts offer alleged surprise, denial, ashamed admission, and blaming of overzealous family members and other “straw men” listed as actual purchasers of the “amplification” services.[296] This setup may offer bot owners plausible deniability in the press, and some celebrities and corporate brands may be unaware of their “guardian angels,” but perhaps more importantly, it seems many people are being dishonest about using social bots online.

If the *New York Times* story helps verify researchers' allegations that there are millions of false accounts online following and supporting individuals and brands,[297] then who is behind them? Who is paying for the many waves of one-star review online attacks reported by businesses?[298] No doubt some is the result of political or pranking users crowdsourcing their online mischief, but that does not exclude the likelihood of bot activity and likely involves some financial incentive behind it all. While bot mischief in political elections has garnered a great deal of deserved alarm, Pew Research reports that most social bots post links to commercial interests, not political.[299]

There is good reason to believe that soliciting, paying for, or even permitting bot-driven online commercial support, reviews, or endorsements may directly or vicariously violate the CA Bot Act. Suffice it to say that attorneys and other advisers should consider having an honest, if diplomatic, discussion with their clients about the legal implications of social amplification services, especially to confirm no one has "gone rogue," as was often claimed (perhaps incredulously) by some ***893** of the famous actors, pundits, chefs, and models benefitting from bot followers in the *New York Times* article.

With so many consumers acting on bad information, the time may be ripe for a concerted effort to tear away the mask of just who is shoveling the BS (bot speech).

As to the political component, bots are empowering a pervasive and sinister effort to exploit social conflict and showcase a distorted view of political division by giving voice to the most extreme, hostile, and uncompromising views. Such behavior contributes to apathy, a degradation of the national conversation and a poor feedback loop to measure actual constituent interest. The declared intent by foreign actors to interfere with political elections in the United States has been confirmed by various governmental and intelligence agencies. There can be no doubt more is coming in upcoming elections.

China has professionalized the weaponization of social media to advance a viewpoint and promote online discord. Chinese companies give training seminars to government representatives from Mexico to the Middle East in the use of "big data public-opinion management systems [and] tools for real-time monitoring of negative public opinion and a positive energy public-opinion guidance system."[300]

Worldwide, social media has quickly proven a popular Western export, and bots have attacked opponents in the United Kingdom's "Brexit" and Spain's Catalonia referendums,[301] influenced political elections in France, Germany, Austria and Italy,[302] and used smoke screening to spread "fake news"[303] in political discussions from Japan[304] ***894** to India[305] to South Africa[306] to Brazil.[307] Twitter had to take down a Saudi Arabian botnet that diminished the Kingdom of Saudi Arabia's role in the disappearance of journalist Jamal Khashoggi.[308]

And while Russian bot activity has earned a well-documented notoriety in the United States, bots have been used by political actors of all kinds *along the political spectrum* across the globe. During the 2017 election in Britain, which saw the highest youth turnout in nearly two decades, two young British political activists allegedly created a bot to take over thousands of real Tinder accounts and flirt with real users, chatting and steering the conversation to politics and virtues of the Labour Party.[309]

With the use of malicious bots now a worldwide epidemic, the CA Bot Act, as a regulatory response, may prove itself a test case not only for the United States but for the whole world. Both technological and legal obstacles may temper overly arduous or impatient expectations. But a path to action lies ahead for the motivated. And in the struggle by humans against deceptive online robots, the legislative history states it best: the CA Bot Act arrives to "start the process of drawing legal lines in the sand and provide mechanisms for human users to join the battle."[310]

Footnotes

a1 JD, New York University Law School; MFA, New York University Tisch School of the Arts. The Author is an attorney, policy writer, and filmmaker in California.

1 *See SB-1001 Bots: Disclosure*, Cal. Legis. Info., https://leginfo.legislature.ca.gov/faces/billHistoryClient.xhtml?bill_id=201720180SB1001 [https://perma.cc/K3QPM8CH] (last visited Apr. 1, 2020).

2 Katina Michael, *Bots Without Borders: How Anonymous Accounts Hijack Political Debate*, Conversation (Jan. 23, 2017, 10:25 PM), https://theconversation.com/bots-without-borders-how-anonymous-accounts-hijack-political-debate-70347 [https://perma.cc/M58P-K5XV].

3 *Id.* A taxonomy of bots in use is provided. *Id.*

4 Cal. Bus. & Prof. Code § 17941(a) (West 2019).

5 *Id.* For an in-depth discussion of federal and state laws regulating the use of online bots for ticket scalping, see *infra* Section III.B.1.b.

6 Stefan Wojcik et al., *Bots in the Twittersphere*, Pew Res. Ctr.: Internet & Tech. (Apr. 9, 2018), https://www.pewresearch.org/internet/2018/04/09/bots-in-the-twittersphere/ [https://perma.cc/H427-PV7N].

7 *See* Stan Franklin & Art Graesser, *Is It an Agent, or Just a Program?: A Taxonomy for Autonomous Agents*, 1996 Proc. Workshop on Intelligent Agents III: Agent Theories, Architectures, & Languages 21, 22.

8 *See* A. M. Turing, *Computing Machinery and Intelligence*, 59 Mind 433, 434 (1950). Computing pioneer Alan Turing replaced asking whether machines can think with evaluating the success of artificial intelligence based on how well the computer can convince someone it is in fact a person. *See id.*

9 *See 80% of Businesses Want Chatbots by 2020*, Bus. Insider (Dec. 14, 2016, 9:15 AM), https://www.businessinsider.com/80-of-businesses-want-chatbots-by-2020-2016-12 [https://perma.cc/E6AA-GSTK].

10 1 Robert S. Mueller, III, Report on the Investigation into Russian Interference in the 2016 Presidential Election 15-16 (2019).

11 *See* Chris Baraniuk, *How Twitter Bots Help Fuel Political Feuds*, Sci. Am. (Mar. 27, 2018), https://www.scientificamerican.com/article/how-twitter-bots-help-fuel-politicalfeuds/ [https://perma.cc/ZC2Y-XBYL].

12 Senate Judiciary Comm., SB 1001 Bill Analysis 1 (2018), https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201720180SB1001 [https://perma.cc/MC53-RS98].

13 Elisabeth Eaves, *The California Lawmaker Who Wants to Call a Bot a Bot*, Bull. Atomic Scientists (Aug. 23, 2018), https://thebulletin.org/2018/08/the-california-lawmaker-whowants-to-call-a-bot-a-bot/ [https://perma.cc/U4G5-M6AB].

14 *See* Assembly Comm. on Arts, Entmn't, Sports, Tourism, & Internet Media, SB 1001 Bill Analysis 1 (2018), https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201720180SB1001 [https://perma.cc/MMD2-TVGW].

15 Mark R. Warner, Potential Policy Proposals for Regulation of Social Media and Technology Firms 8 (2018) (draft white paper), https://www.warner.senate.gov/public/_cache/files/d/3/d32c2f17-cc76-4e11-8aa9-897eb3c90d16/65A7C5D983F899DAAE5AA21F57BAD944.social-media-regulation-proposals.pdf [https://perma.cc/8EVJ-46UV]. Partly based on US Senator Mark Warner's 2018 policy paper recommending Congress regulate social media "to clearly and conspicuously label" bots and require internet platform providers "to identify and curtail inauthentic accounts." *Id.*

16 *What Is a DMCA Takedown?*, DMCA (Oct. 1, 2019), https://www.dmca.com/faq/Whatis-a-DMCA-Takedown [https://perma.cc/F7K8-EZL4].

17 *See* Jamie Williams & Jeremy Gillula, *Victory! Dangerous Elements Removed from California's Bot-Labeling Bill*, Electronic Frontier Found. (Oct. 5, 2018), https://www.eff.org/deeplinks/2018/10/victory-dangerous-elements-removed-californias-bot-labeling-bill [https://perma.cc/BE58-TVEJ]. The Electronic Frontier Foundation worked with Senator Hertzberg to remove the CA Bot Act's takedown system and tailor the language to limit its First Amendment impact. *Id.*

18 By contrast, US Senate Bill 3127 would require "social media provider[s] to establish and implement policies and procedures to require a user of a social media website owned or operated by the social media provider to publically [sic] disclose the use of any automated software program or process intended to impersonate or replicate human activity online on the social media website." Bot Disclosure and Accountability Act of 2018, S. 3127, 115th Cong. § 4 (2018).

19 *See* Madeline Lamo & Ryan Calo, *Regulating Bot Speech*, 66 UCLA L. Rev. 988, 989 (2019) (providing a comprehensive examination of bot disclosure via an earlier draft of Senate Bill 1001). This Article owes much to Calo and Lamo's work, especially in speech-regulation law.

20 *See infra* Part IV.

21 *See* Off. of Att'y Gen.: Xavier Becerra, https://oag.ca.gov/ [https://perma.cc/BSP6-QAH7] (last visited Apr. 3, 2020) [hereinafter Off. Att'y Gen.].

22 Cal. Bus. & Prof. Code § 17200 et seq. (West 2019).

23 Cal. Civ. Code §§ 1709-10 (West 2019).

24 *Id.* The UCL is a strict-liability statute, and it may sanction misleading representations in commerce, even without an intent to deceive. However, proving a violation of the UCL requires that *all* elements of the "borrowed statute" be violated, including intent. *Id.*

25 *See, e.g.*, Cairo, Inc. v. Crossmedia Servs., Inc., No. C 04-04825 JW, 2005 WL 756610 (N.D. Cal. Apr. 1, 2005) (holding that an online research firm assented to a website's terms of service agreement by its use of an information-gathering bot ('spider') that frequented the website).

26 *See, e.g.*, Voyeur Dorm, L.C. v. City of Tampa, 265 F.3d 1232 (11th Cir. 2001) (holding that an adult website did not violate a residential zoning code because viewers were not actually present when nudity was displayed).

27 *See, e.g.*, Carris v. Marriott Int'l, Inc., 466 F.3d 558, 561 (7th Cir. 2006) (holding that Bahamian law governed an Illinois state tort case over a jet ski accident in the Bahamas, despite the trip being booked on a computer in Illinois).

28 *See, e.g.*, Sidney A. Rosenzweig, Comment, *Don't Put My Article Online!: Extending Copyright's New-Use Doctrine to the Electronic Publishing Media and Beyond,* 143 U. Pa. L. Rev. 899, 900 (1995).

29 *See, e.g.*, Long v. Marubeni Am. Corp., No. 05Civ.639(GEL)(KNF), 2006 WL 2998671, at *4 (S.D.N.Y. Oct. 19, 2006) (holding that an employee waived their attorney-client privilege and had no expectation of privacy in emails sent, even with a personal password-protected email account, because they were sent on a company internet portal, which created a copy of it accessible to the company).

30 *See, e.g.*, Zeran v. Am. Online, Inc., 129 F.3d 327 (4th Cir. 1997) (holding that defendant-ISP AOL was immune under section 230 for publishing defamatory statements and personal details of plaintiff resulting in harassment and death threats).

31 *See, e.g.*, Chi. Lawyers' Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc., 519 F.3d 666 (7th Cir. 2008) (holding that Craigslist was not liable for third-party users' discriminatory housing ads).

32 Dennis T. Yokoyama, *You Can't Always Use the* Zippo *Code: The Fallacy of a Uniform Theory of Internet Personal Jurisdiction*, 54 DePaul L. Rev. 1147, 1164 (2005).

33 *No Bad Puns: A Different Approach to the Problem of Personal Jurisdiction and the Internet*, 116 Harv. L. Rev. 1821, 1821 (2003) (critiquing the still-applicable *Zippo* standard for long-arm personal jurisdiction where a defendant's online presence constitutes minimum contacts with the state).

34 Renee DiResta, *A New Law Makes Bots Identify Themselves--That's the Problem*, Wired (July 24, 2019, 9:00 AM), https://www.wired.com/story/law-makes-bots-identify-themselves/ [https://perma.cc/YTL2-VHQF].

35 *Id.* Some bots are hybrids--social bots with chatbots' ability to converse--but for purposes of this Article they will be analyzed separately.

36 *Id.* Haling out-of-state CA Bot Act violators into court remains in doubt. *Id.* A rehabilitation of *Calder v. Jones,* and its "express aiming requirement" that the defendant directed conduct *specifically toward* the forum state, has shifted California jurisprudence away from finding minimum contacts for online posting *accessible* in California but *conducted* out of state--a trend continued in *Burdick v. Superior Court*, where defendant's only ties with California consisted of having posted allegedly defamatory statements *on a personal Facebook page. See* Calder v. Jones, 465 U.S. 783 (1984); Burdick v. Superior Court, 183 Cal. Rptr. 3d 1 (Cal. Ct. App. 2015).

37 Cal. Bus. & Prof. Code § 17941(a) (West 2019).

38 *Id.* § 17941(b).

39 *See, e.g.*, Patterson v. New York, 432 U.S. 197, 211 (1977).

40 Off. of Att'y Gen., *supra* note 21. As of January 2020, the California attorney general has not indicated an intention to enforce the CA Bot Act. *Id.*

41 Jones v. Superior Court, 372 P.2d 919, 925 (Cal. 1962) (Peters, J., concurring in part and dissenting in part) ("[U]ntil the prosecution has made out a prima facie case against [the defendant,] he is not and should not be compelled to assist the prosecution either in its case in chief or in rebuttal of his possible defense.").

42 *See* Speiser v. Randall, 357 U.S. 513 (1958).

43 *See* Assembly Comm. on Arts, Entmn't, Sports, Tourism, & Internet Media, *supra* note 14, at 1; Senate Comm. on Bus., Professions & Econ. Dev., SB 1001 Bill Analysis 2 (2018), https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201720180SB1001 [https://perma.cc/93FZ-2CBR]; Senate Judiciary Committee, *supra* note 12, at 4. The statute's definition of "bot" evolved from "a machine, device, computer program, or other computer software that is designed to mimic or behave like a natural person such that a reasonable natural person is unable to discern its artificial identity," to "an online account that is either automated or designed to mimic or behave like the account of a natural person," to "an automated online account where all or substantially all of the actions or posts of that account are not the result of a person." *See* Assembly Comm. on Arts, Entmn't, Sports, Tourism, & Internet Media, *supra* note 14, at 1; Senate Comm. on Bus., Professions & Econ. Dev., *supra*, at 2; Senate Judiciary Committee, *supra* note 12, at 4.

44 Jonah Engel Bromwich, *Bots of the Internet, Reveal Yourselves!*, N.Y. Times (July 16, 2018), https://www.nytimes.com/2018/07/16/style/how-to-regulate-bots.html [https://perma.cc/297W-FAF4].

45 Franklin & Graesser, *supra* note 7, at 22.

46 Cal. Bus. & Prof. Code § 17940(a) (West 2019). "Person" is defined to include "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." Bus. & Prof. § 17940(d).

47 *See, e.g., id.*; Franklin & Graesser, *supra* note 7, at 22 ("'Persistent' distinguishes agents from subroutines; agents have their own ideas about how to accomplish tasks.").

48 *See, e.g.*, Cal. Bus. & Prof. Code § 17940. Bots are frequently designed and licensed by software developers or available online as freeware, and a bot's *user* may not have designed or own its underlying software. Kurt Wagner, *Bots, Explained*, Vox (Apr. 11, 2016, 5:00 AM), https://www.vox.com/2016/4/11/11586022/what-are-bots [https://perma.cc/949X-V9TY]. However, to avoid the ambiguity of the term *bot user*, which might refer to a human unwittingly interacting with a bot, this Article refers to a potential violator of the CA Bot Act as a bot's *owner*.

49 Christian Grimme et al., *Social Bots: Human-Like by Means of Human Control?*, 5 Big Data (Special Issue) 279 (2017). Bot activity could conceivably constitute *interacting but not communicatin*g with human users--for example, installing software on a human user's device. *Id.* But that activity would only be proscribed if the bot *intends to mislead* the human user, which impliedly involves the user being led by the bot. *Id.* That is, interactions between a human and bot will usually involve some textual or visual media exchange--email, text, online comment, or public social network behavior--that arguably qualifies as communication. *Id.* Therefore, for brevity, this Article treats the term "interacts" as a catchall and refers to bot "communication" inclusive of noncommunicative interaction.

50 Cal. Bus. & Prof. Code § 17941(a) (emphasis added).

51 Christopher Olston & Marc Najork, *Web Crawling*, 4 Found. & Trends Info. Retrieval 175, 176 (2010). Data mining is the process of sifting through electronic information to observe patterns and derive knowledge from the data. *See What Is Data Mining*, IGI Global, https://www.igi-global.com/dictionary/challenges-opportunities-soft-computing-tools/6763 [https://perma.cc/S8X8-YN7V] (last visited Apr. 5, 2020). Computers can do so much more quickly than humans, and bots have been used for data mining since business information was first stored on computers. *See* Nagaratna P. Hegde & B. Varija, *Data Mining and MultiAgent Integration*, 2017 Int'l J. Engineering Trends & Tech. (Special Issue) 9, 10.

52 Gautam Pant et al., *Crawling the Web, in* Web Dynamics: Adapting to Climate Change in Content, Size, Topology and Use 153, 173 (Mark Levene & Alexandra Poulovassilis eds., 2004). The earliest use of online bots was to automatically host channels on a text-

based messaging platform known as Internet Relay Chat that gained prominence in 1988. *See* Todd Biske, Google: Groups (Nov. 14, 1991), https://groups.google.com/forum/#!topic/alt.irc/qZyM6-H_QMQ [https://perma.cc/2QKS-DZNK].

53 Pant et al., *supra* note 52, at 154. Web crawlers start with a list of hyperlinks known as "seeds," then add links they encounter to a list and fetch them. *Id.* at 153.

54 *See, e.g.*, Seyed M. Mirtaheri et al., *A Brief History of Web Crawlers*, 2013 Proc. Conf. Ctr. for Advanced Stud. on Collaborative Res. 40, 40.

55 *Id.* at 43.

56 *Id.* at 44. Googlebot and Bingbot are the two most common search-engine web crawlers, powering their respective search engines. Brian Jackson, *Web Crawlers and User Agents--Top 10 Most Popular*, KeyCDN, https://www.keycdn.com/blog/web-crawlers [https://perma.cc/LHA2-MXD6] (last updated June 6, 2017).

57 Klint Finley, *'Scraper' Bots and the Secret Internet Arms Race*, Wired (July 23, 2018, 7:00 AM), https://www.wired.com/story/scraper-bots-and-the-secret-internet-arms-race/ [https://perma.cc/3KHN-P4ZQ].

58 Cody Gette, *Two (and a Half) Ways to Get Weather Data: Part 1--Web Scraping from Wunderground*, C. R. Gette (Apr. 21, 2018), https://gettecr.github.io/wunderground-scraping.html#.XnQ0hZNKg0p [https://perma.cc/TKN6-LBA2].

59 *See, e.g.*, Cornell L. Sch.: Legal Info. Inst., https://www.law.cornell.edu/ [https://perma.cc/VV65-9HYH] (last visited Apr. 5, 2020) (providing statutory and case law online for free access).

60 *See* Ruxandra Mindruta, *The Top Social Media Monitoring Tools*, Brand watch (Sept. 27, 2019), https://www.brandwatch.com/blog/top-social-media-monitoring-tools/ [https://perma.cc/7TGE-CDNT].

61 *See* Google Scholar, https://scholar.google.com/ (last visited Apr. 5, 2020) (an online searchable index for published scholarly articles and case law).

62 The European Union's 2018 General Data Protection Regulation regulates online scraping, with an emphasis on privacy protection. Commission Regulation 2016/679, 2016 O.J. (L 119) 1. But no specific law exists in the United States. *See* William S. Galkin, *The State of the Law on Data Scraping*, Galkin Law: Blog (Sept. 26, 2017), http://blog.galkinlaw.com/weblaw-scoutblog/legality-of-data-scraping [https://perma.cc/R6CH-JD3K]. Cases have varied; a California appellate court ruled that scraping is legal, although bypassing online security might not be. *See* hiQ Labs, Inc. v. LinkedIn Corp., 273 F. Supp. 3d 1099, 1103 (N.D. Cal. 2017), *aff'd,* 938 F.3d 985 (9th Cir. 2019). For a defense of scraping's mutual benefits in the exchange of information, see generally Jeffrey Kenneth Hirschey, *Symbiotic Relationships: Pragmatic Acceptance of Data Scraping*, 29 Berkeley Tech. L.J. 897 (2014).

63 Finley, *supra* note 57.

64 *See* Julien Picot, *An Introduction to Web Crawler*, Oncrawl: Blog (Mar. 8, 2016), https://www.oncrawl.com/technical-seo/introduction-web-crawler/ [https://perma.cc/7EBA-GF7W]. Crawlers do relay data to the bot owner who dispatched them, but there is no deception involved. *See id.*

65 *See generally* Huma Shah et al., *Can Machines Talk? Comparison of Eliza with Modern Dialogue Systems*, 58 Computers Hum. Behav. 278 (2016).

66 These terms are used in conflict, even in academic literature, though for many users and sellers, personal assistants are disembodied audio chatbots that perform tasks for the user (play music, make calls), represented by Apple's Siri, Amazon's Alexa, and so on. *See id.*

67 Huma Shah, *A.L.I.C.E.: An ACE in Digitaland*, 4 triple C: Comm., Capitalism & Critique 284, 284-85 (2006). Shah's research is an early example of chatbot technology. *See id.*

68 NLP uses a database of words in a hierarchy of value to recognize patterns and teach computers how to recognize, interpret, and respond to human language in kind. *See* Jason Brownlee, *What Is Natural Language Processing?*, Machine Learning Mastery: Blog (Sept. 22, 2017), https://machinelearningmastery.com/natural-language-processing/ [https://perma.cc/J5FL-2DCN].

69 *See* Cal. Bus. & Prof. Code § 17941 (West 2019); Nicole Radziwill & Morgan Benton, Evaluating Quality of Chatbots and Intelligent Conversational Agents (2017) (unpublished manuscript), https://arxiv.org/pdf/1704.04579.pdf [https://perma.cc/A9PT-J6PP].

70 *See* Alisa Kongthon et al., *Implementing an Online Help Desk System Based on Conversational Agent*, 2009 Proc. Int'l Conf. on Mgmt. Emergent Digital Ecosystems. 450, 450.

71 Oracle, Can Virtual Experiences Replace Reality? (2016), https://www.oracle.com/webfolder/s/delivery_production/docs/FY16h1/doc35/CXResearchVirtualExperiences.pdf [https://perma.cc/EDT7-G5F2].

72 Rachita Rake & Supradip Baul, Allied Mkt. Research, Chatbot Market in BFSI by Platform, Type and End User: Global Opportunity Analysis and Industry Forecast, 2018-2024 (2018).

73 Yvon Moysan & Jade Zeitoun, *Chatbots as a Lever to Redefine Customer Experience in Banking*, 3 J. Digital Banking 242 (2019).

74 Supratip Ghose & Jagat Joyti Barua, *Toward the Implementation of a Topic Specific Dialogue Based Natural Language Chatbot as an Undergraduate Advisor*, Int'l Conf. on Informatics, Electronics & Vision Proc., 2013, at 1, 1.

75 *See* DoNotPay, https://donotpay.com/ (last visited Apr. 6, 2020) (a website, now an app, allowing users to appeal parking tickets). *See also NRF Parker Chatbots*, Norton Rose Fulbright (Apr. 2019), https://www.nortonrosefulbright.com/en/knowledge/publications/b3667e00/nrf-parker [https://perma.cc/2D3R-AUFR] (a law-firm chatbot developed to give basic answers to questions about changes to the law on data protection and privacy).

76 *See, e.g., Chatbot Survey Taking-The Future Is Now*, Survey Police (Sept. 25, 2018), https://www.surveypolice.com/blog/chatbot-survey-taking-the-future-is-now/ [https://perma.cc/VFR6-KP4H]. "U-Report is a free tool for community participation, designed to address issues that the population cares about" by collecting and communicating needs and messages back and forth from the community to UNICEF. *About U-Report*, U-Report, https://ureport.in/about/ [https://perma.cc/TB4N-BG9X] (last visited Mar. 20, 2020).

77 *ChatBots for Senior People and Patients with Alzheimer's Disease*, Endurance Robots, http://endurancerobots.com/azbnmaterial/chatbots-for-senior-people-and-patients-with-alzheimer-s-disease/ [https://perma.cc/6R3Q-38KY] (last visited Mar. 20, 2020).

78 Nick Romeo, *The Chatbot Will See You Now*, New Yorker (Dec. 25, 2016), https://www.newyorker.com/tech/annals-of-technology/the-chatbot-will-see-you-now [https://perma.cc/U69V-R2JS] (describing "Karim--a psychotherapy chatbot designed by X2AI, an artificial-intelligence startup in Silicon Valley," which acts as a grief counselor to Syrian refugees).

79 *See generally* Shah et al., *supra* note 65.

80 *Social Media Fact Sheet*, Pew Res. Ctr.: Internet & Tech. (June 12, 2019), https://www.pewresearch.org/internet/fact-sheet/social-media/ [https://perma.cc/46GY-BK73]. The Pew Research Center began tracking social media adoption in 2005, at which point just 5 percent of US adults used at least one social networking platform. *Id.* By 2018 that number had more than tripled to 70 percent, rising to 88 percent in adults under the age of twenty-nine. Growth is now mostly fed by younger users. *Id.*

81 "Social bot" refers to the imitation of social interaction, not to social media. *See* Emilio Ferrara et al., *The Rise of Social Bots*, 59 Comms. ACM 96, 96 (2016).

82 Yazan Boshmaf et al., *Design and Analysis of a Social Botnet*, 57 Computer Networks 556, 556 (2013).

83 Mirkin v. Wasserman, 858 P.2d 568, 578 (Cal. 1993) (holding that misleading cereal ads shown to children were the cause of their parents' purchase). "It should be sufficient that defendant makes a misrepresentation to one group *intending to influence the behavior of the ultimate purchaser*, and that he succeeds in this plan." *Id.* (quoting Comm. on Children's Television, Inc. v. Gen. Foods Corp., 673 P.2d 660, 674 (Cal. 1983)) (emphasis added).

84 *Id.* at 575 (quoting Restatement (Second) of Torts § 533 (Am. Law Inst. 1977)).

85 The federal Better Online Ticket Sales (BOTS) Act (targeting online ticket-purchasing bots) bans bots from circumventing cybersecurity measures; the Computer Fraud and Abuse Act (CFAA) similarly prohibits "knowingly and with intent to defraud, access[ing] a protected computer without authorization, or exceed[ing] authorized access, and by means of such conduct furthers

the intended fraud and obtains anything of value." 15 U.S.C. § 45c(a)(1)(A) (2018) ("[I]t shall be unlawful for any person ... to circumvent a security measure, access control system, or other technological ... measure on an Internet website or online service that is used by the ticket issuer to enforce ... event ticket purchasing limits or to maintain the integrity of posted online ticket purchasing order rules."); 18 U.S.C. § 1030(a)(4) (2018).

86 Cal. Bus. & Prof. Code § 17941(a) (West 2019) (stating that it is "unlawful ... 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").

87 Ian R. Kerr, *Bots, Babes and the Californication of Commerce*, 1 U. Ottawa L.& Tech. J. 285, 303-05 (2004).

88 *See generally* Turing, *supra* note 8; *see also The Loebner Prize*, U. Cal.--Berkeley: Computer Intelligence & Turing Test, https://www.ocf.berkeley.edu/~arihuang/academic/research/loebner.html [https://perma.cc/S5TX-SE2W] (last visited Apr. 7, 2020) (describing the process--which, although criticized for a lack of rigor, remains popular--by which judges interact with both anonymous human "confederates" and AI chatbots and must guess which is human).

89 *See, e.g.*, Robert Dale, *The Return of the Chatbots*, 22 Nat. Language Engineering 811, 814 (2016) (for instance, "Sorry I didn't understand that").

90 One study found 63 percent of users interact with AI without knowing they are conversing with a chatbot. *See* Mimi An, *Artificial Intelligence Is Here--People Just Don't Realize It*, HubSpot (Jan. 30, 2017, 10:00 AM), https://blog.hubspot.com/marketing/artificial-intelligence-is-here [https://perma.cc/P58B-BBVY]; *see also* Anbang Xu et al., *A New Chatbot for Customer Service on Social Media*, 2017 Proc. CHI Conf. on Hum. Factors Computing Systems 3506, 3506.

91 Petter Bae Brandtzæg & Asbjørn Følstad, *Why People Use Chatbots*, 4 Int'l Conf. on Internet Sci. Proc. 377, 387 (2017) (describing reports saying, "[T]here's a sense of talking to someone when I use them. It's almost like you are talking to a real person," and "I know they aren't real but it feels like it is").

92 *See* Xu et al., *supra* note 90, at 3506.

93 Rick Ramos, *Screw the Turing Test--Chatbots Don't Need to Act Human*, Venture Beat (Feb. 3, 2017, 12:10 PM), https://venturebeat.com/2017/02/03/screw-the-turing-test-chatbots-dont-need-to-act-human/ [https://perma.cc/5RL3-AJ52].

94 *See* Ross A. Lincoln, *Fans Are Really Emotional About C-3PO After 'Star Wars: The Rise of Skywalker' Final Trailer*, The Wrap (Oct. 21, 2019, 9:17 PM), https://www.thewrap.com/fans-are-really-emotional-about-c-3po-after-star-wars-the-rise-of-skywalker-finaltrailer/ [https://perma.cc/6HA6-YZTK]. *But see* Masahiro Mori, *The Uncanny Valley*, IEEE Robotics & Automation Mag., June 2012, at 98, 99-100.

95 This Author thanks the editor in chief of the *Vanderbilt Journal of Entertainment and Technology Law*, Jin Yoshikawa, for identifying this idea, which he called "good chatbots."

96 *See* Romeo, *supra* note 78 (describing "Karim"--a psychotherapy chatbot that acts as a grief counselor to Syrian refugees).

97 Sylvia McKeown, *Chatbot rAInbow Gives Abused Women a Nonjudgmental 'Friend' to Lean on*, Sunday Times (Feb. 3, 2019, 12:07 AM), https://www.timeslive.co.za/sunday-times/lifestyle/2019-02-03-chatbot-rainbow-*gives-abused-women-a-nonjudgmental*-friend-*to-lean*-on/ [https://perma.cc/KX3Z-UMCK]; *see also* Romeo, *supra* note 78.

98 *See* Paul Blumenthal, *How a Twitter Fight over Bernie Sanders Revealed a Network of Fake Accounts*, Huff Post Pol. (Mar. 14, 2018, 5:45 AM), https://www.huffpost.com/entry/democratic-bot-network-sally-albright_n_5aa2f548e4b07047bec68023 [https://perma.cc/A2RA-MU2H] (describing Twitter accounts that displayed scraped photographs of models, athletes, other accounts, and crime victims).

99 Stefan Stieglitz et al., *Do Social Bots Dream of Electric Sheep? A Categorisation of Social Media Bot Accounts*, Australasian Conf. on Info. Syss. Proc., 2017, at 1, 3, 6.

100 Kai-Cheng Yang et al., *Arming the Public with Artificial Intelligence to Counter Social Bots*, 1 Hum. Behav. & Emerging Techs. 48, 49 (2019).

101 Engalla v. Permanente Med. Grp., Inc., 938 P.2d 903, 917 (Cal. 1997) (quoting Yellow Creek Logging Corp. v. Dare, 30 Cal. Rptr. 629, 632 (Dist. Ct. App. 1963)); *see also* Gagne v. Bertran, 275 P.2d 15, 20 (Cal. 1954) (An intent to mislead can be inferred from the defendant's making "a [misrepresentation] with knowledge [the plaintiff] would act in reliance thereon").

102 *See* Cal. Civ. Code § 1710(3) (West 2019).

103 "Phishing" generally refers to malicious online efforts (spam emails, malware, etc.) to gain a user's personal data, often by casting a wide "net"; "spear-phishing" is such activity *targeted* at a specific user; social media facilitates finding targets and gaining their trust. Nena Giandomenico, *What Is Spear-Phishing? Defining and Differentiating Spear-Phishing from Phishing*, Digital Guardian: Data Insider (Oct. 24, 2019), https://digitalguardian.com/blog/what-is-spear-phishing-defining-and-differentiating-spear-phishing-and-phishing [https://perma.cc/FRC5-WMX2].

104 Tim Hwang et al., *Socialbots: Voices from the Fronts*, Interactions, Mar.-Apr. 2012, at 38, 42-43.

105 Kurt Thomas & David M. Nicol, *The Koobface Botnet and the Rise of Social Malware*, 5 Int'l Conf. on Malicious & Unwanted Software Proc. 63, 63 (2010).

106 Yang et al., *supra* note 100, at 49.

107 Civ. § 1710; Linear Tech. Corp. v. Applied Materials, Inc., 61 Cal. Rptr. 3d 221, 234 (Cal. Ct. App. 2007); LiMandri v. Judkins, 60 Cal. Rptr. 2d 539, 543 (Cal. Ct. App. 1997). To prove concealment, the plaintiff must show (i) the defendant was under a duty to disclose to the plaintiff; (ii) the defendant concealed or suppressed a material fact; (iii) the defendant intended to defraud the plaintiff; (iv) the plaintiff would have acted otherwise if aware of the concealed fact; and (v) the plaintiff sustained damage from the concealment of the fact. *Linear Tech. Corp.*, 61 Cal. Rptr. 3d at 234.

108 Cal. Bus. & Prof. Code § 17941 (West 2019).

109 Lesley Fair, *Full Disclosure*, FTC: Bus. Blog (Sept. 23, 2014, 11:32 AM), https://www.ftc.gov/news-events/blogs/business-blog/2014/09/full-disclosure [https://perma.cc/6EDP-5YMN].

110 *See* Assembly Committee on Arts, Entertainment, Sports, Tourism, and Internet Media, *supra* note 14, at 6.

111 *See id.*

112 *See* Nguyen v. Barnes & Noble Inc., 763 F.3d 1171, 1175-77 (9th Cir. 2014). The distinction was first articulated in connection with software licensing agreements. *See* Wall Data, Inc. v. L.A. Cty. Sheriff's Dep't, 447 F.3d 769, 775 nn.4-5 (9th Cir. 2006). "Shrink-wrap" software licensing agreements (bound with plastic "shrink-wrap" in the days when shipped CDs were necessary to install software) were less likely to be noticed by a purchaser and thus less enforceable, as opposed to "click-wrap" (or "click-through") agreements, which requires users to affirmatively agree to be bound by clicking a button to unlock the software once it is installed. *See* Norcia v. Samsung Telecomms. Am., LLC, 845 F.3d 1279, 1289 (9th Cir. 2017). The term "browse-wrap" was coined to describe contractual language offered to a user for passive browsing on the internet. *Nguyen*, 763 F.3d at 1174 (a warning on the web page that "[B]y visiting any area in the [website], creating an account, [or] making a purchase a User is deemed to have accepted the Terms of Use" was deemed insufficient to put the user on notice).

113 *Nguyen*, 763 F.3d at 1178-79 ("[W]here a website makes its terms of use available via a conspicuous hyperlink on every page of the website but otherwise provides no notice to users nor prompts them to take any affirmative action to demonstrate assent, even close proximity of the hyperlink to relevant buttons users must click on--without more--is insufficient to give rise to constructive notice.").

114 *Id.* at 1176 (quoting Be In, Inc. v. Google, Inc., No. 12-CV-03373-LHK, 2013 WL 5568706, at *6 (N.D. Cal. Oct. 9, 2013)) ("The defining feature of browsewrap agreements is that the user can continue to use the website or its services without [seeing] ... the browsewrap agreement or even knowing that such a webpage exists.").

115 Under the UCL, plaintiffs must show "injury in fact ... as a result of" a commercial regulatory violation. Cal. Bus. & Prof. Code § 17204 (West 2019).

116 *See, e.g.*, Mirkin v. Wasserman, 858 P.2d 568, 572 (Cal. 1993).

117 *See, e.g.*, Lazar v. Superior Court, 909 P.2d 981, 984 (Cal. 1996).

118 Case law requires alleging scienter (knowledge a representation is misleading) for fraud, so the bot owner's knowledge must be alleged. *See Mirkin*, 858 P.2d at 584. A user unaware of bot malware on a computer would lack the intent and knowledge needed to violate the CA Bot Act. *See id.*

119 Cal. Bus. & Prof. Code § 17942(a) (West 2019).

120 *Id.* § 17204.

121 *Id.* § 17200.

122 Farmers Ins. Exch. v. Superior Court, 826 P.2d 730, 734 (Cal. 1992).

123 Rose v. Bank of Am., N.A., 304 P.3d 181, 185 (Cal. 2013).

124 Cel-Tech Commc'ns, Inc. v. L.A. Cellular Tel. Co., 973 P.2d 527, 541 (Cal. 1999).

125 Claudia Wrazel & Saskia Kim, Cal. State Legislature, A Primer on Business and Professions Code Section 17200: California's Unfair Competition Law 1 (2003), https://ajud.assembly.ca.gov/sites/ajud.assembly.ca.gov/files/reports/0103%20UCLback-ground.pdf [https://perma.cc/EWB2-VV2K].

126 Mfrs. Life Ins. Co. v. Superior Court, 895 P.2d 56, 71 (Cal. 1995).

127 Solus Indus. Innovations, LLC v. Superior Court, 410 P.3d 32, 47 (Cal. 2018) (holding that California employment standards were not preempted by the federal Occupational Safety and Health Administration and distinguishing *In re* Tobacco Cases II, 163 P.3d 106 (Cal. 2007), which held that federal laws governing tobacco preempted a UCL claim for the violation of state laws concerning tobacco advertisements to minors).

128 *Id.* at 35.

129 Cal. Bus. & Prof. Code §§ 17941(a), 17942(a) (West 2019).

130 In June 2018, Senator Diane Feinstein introduced Senate Bill 3127 (Bot Disclosure and Accountability Act of 2018), which would require social media providers and others to "disclose the use of any automated software program or process intended to impersonate or replicate human activity online on the social media website." Bot Disclosure and Accountability Act of 2018, S. 3127, 115th Cong. § 4(b) (2018). The law has not been adopted, and its future remains unclear. *S.3127--Bot Disclosure and Accountability Act of 2018*, Congress.gov, https://www.congress.gov/bill/115th-congress/senate-bill/3127/all-actions?overview=closed&KWICView=false [https://perma.cc/J7UD-AQ2J] (last visited Mar. 18, 2020).

131 BOTS Act of 2016, S. 3183, 114th Cong. § 2(a)(1)(A) (2016).

132 *Id.*

133 Cal. Bus. & Prof. Code § 17941(a) (West 2019).

134 *Compare* Cal. Civ. Code § 1572 (West 2019) (titled "Actual Fraud"), *with* Cal. Civ. Code § 1710 (West 2019) (titled "Deceit Defined"). Fraudulent deceit and actual fraud are subject to the same legal principles, and this Article's analysis should be understood as applicable to both statutes. *See, e.g.*, Stone v. Farnell, 239 F.2d 750, 754 (9th Cir. 1956); Sixta v. Ochsner, 9 Cal. Rptr. 617, 620 (Dist. Ct. App. 1960). But since section 1572 focuses on deceit *between two contracting parties*, and much of the bot speech considered here involves speakers and listeners without contractual privity, this Article focuses on sections 1709 and 1710.

135 Cal. Civ. Code § 1709 (West 2019).

136 *Id.* § 1710(3).

137 SCC Acquisitions Inc. v. Cent. Pac. Bank, 143 Cal. Rptr. 3d 711, 715 (Ct. App. 2012) (quoting Blickman Turkus, LP v. MF Downtown Sunnyvale, LLC, 76 Cal. Rptr. 3d 325, 331 (Ct. App. 2008)).

138 Although California's economic-loss rule often limits claims of concealment in commercial transactions to "remedies at contract," punitive damages may be granted when the concealment constituted its own independent tort. *See* Robinson Helicopter Co. v. Dana Corp., 102 P.3d 268, 272 (Cal. 2004). Noneconomic injuries, like harm under the "political prong," are unaffected by the rule. *See id.* at 276.

139 *Compare* Cal. Bus. & Prof. Code § 17200 (West 2019), *with* Cal. Civ. Code § 1710.

140 *See, e.g.*, Corey Varma, Comment, *The Presumption of Injury: Giving Data Breach Victims "A Leg to Stand On"*, 32 J. Marshall J. Info. Tech. & Privacy L. 301, 304 (2016).

141 For example, the "case or controversy" language in the US Constitution's Article III justiciability clause limits the ability of federal courts to hear and decide purported grievances. *See* U.S. Const. art. III, § 2, cl. 1; Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992) ("[T]he core component of standing is an essential and unchanging part of the case-or-controversy requirement of Article III.").

142 *See, e.g.*, Weatherford v. City of San Rafael, 395 P.3d 274, 278 (Cal. 2017).

143 *See, e.g.*, Nationwide Biweekly Admin., Inc. v. Superior Court, 234 Cal. Rptr. 3d 468, 471 (Ct. App. 2018), *cert. granted*, 426 P.3d 302 (Cal. 2018). The California Supreme Court will examine whether such public civil actions under the UCL afford a right to a jury trial. *See Nationwide Biweekly Admin.*, 426 P.3d 302; *Nationwide Biweekly Admin.*, 234 Cal. Rptr. 3d. at 488.

144 *See, e.g.*, Solus Indus. Innovations, LLC v. Superior Court, 410 P.3d 32, 35 (Cal. 2018) (action brought by the Orange County district attorney under the UCL based on ("borrowing") the defendant-employer's alleged violations of workplace safety standards established by California's state occupational safety and health law).

145 *See* Kowalsky v. Hewlett-Packard Co., 771 F. Supp. 2d 1138, 1147 (N.D. Cal. 2010) (quoting Cortez v. Purolator Air Filtration Prods. Co., 999 P.2d 706, 717 (Cal. 2000)) ("[B]oth the California Supreme Court and appellate courts have stated that the statute 'imposes strict liability.'"), *vacated in part on other grounds*, 771 F. Supp. 2d 1156 (N.D. Cal. 2011).

146 *See, e.g.*, Grosset v. Wenaas, 175 P.3d 1184, 1196 n.13 (Cal. 2008).

147 California residents had standing to sue for a writ ordering the government to enforce environmental laws. *See* Save the Plastic Bag Coal. v. City of Manhattan Beach, 254 P.3d 1005, 1013 (Cal. 2011) (concluding that a party's interest "in having the laws executed and the duty in question enforced" is sufficient and no showing of "legal or special interest" is necessary); *see also* Bd. of Soc. Welfare v. L.A. Cty., 162 P.2d 627, 628-29 (Cal. 1945).

148 *See* Perry v. Brown, 265 P.3d 1002, 1007 (Cal. 2011) (holding that a gay-marriage opponent activist group had standing to sue for a writ enforcing California's Department of Justice to defend struck down legislation banning gay marriage).

149 *See* Weatherford v. City of San Rafael, 395 P.3d 274, 279 (Cal. 2017).

150 "White knighting" is a popular term of disparagement for users who come to others' rescue in online forums. *White Knight*, Know Your Meme, https://knowyourmeme.com/memes/white-knight [https://perma.cc/V5KT-YY23] (last visited Mar. 20, 2020).

151 *See Weatherford*, 395 P.3d at 278.

152 *See, e.g.*, People *ex rel.* Becerra v. Superior Court, 240 Cal. Rptr. 3d 250, 261 (Ct. App. 2018) (holding that there is "no general 'public interest' exception to the requirement of standing").

153 Solus Indus. Innovations, LLC v. Superior Court, 410 P.3d 32, 47 (Cal. 2018).

154 The bill's original sponsors were Common Sense Media, a consumer group promoting safe and honest media for children, and the Center for Human Technology, an advocacy group founded by former tech employees to promote humane values in the development of new technology. Bromwich, *supra* note 44.

155 California ex rel. Van de Kamp v. Texaco, Inc., 762 P.2d 385, 399 (1988).

156 *Id.*; *see also* Hewlett v. Squaw Valley Ski Corp., 63 Cal. Rptr. 2d 118, 130, 141 (Cal. Ct. App. 1997).

157 *See* People v. Overstock.com, Inc., 219 Cal. Rptr. 3d 65, 86 (Cal Ct. App. 2017) (deeming $6,828,000 as not excessive where an online vendor's misleading prices were treated as repeated violations for as long as they were published online).

158 A number of misrepresentations are embodied by a commercial-prong violation. *See* Cal. Bus. & Prof. Code § 17941 (West 2019). A deceptive social bot posting "verified purchaser" product reviews effectively represents (i) it is a real person, (ii) that bought the product, (iii) it has a given opinion, and (iv) it is objective. *See id.*

159 *See id.* § 17941(a). The UCL is concerned with "business activity," and it does not appear that a CA Bot Act violation "to influence a vote" would be enjoinable under the UCL's borrowing doctrine. *See* Farmers Ins. Exch. v. Superior Court, 826 P.2d 730, 734 (Cal. 1992).

160 Cal. Bus. & Prof. Code § 17204 (West 2019).

161 The UCL was originally drafted to address business name infringement, but in 1963 the California legislature expanded it widely to focus on consumer protection, allowing private actions "acting for the interests of itself, its members *or the general public* .... without individualized proof of deception, reliance and injury" by the specific plaintiff. *See* Comm. on Children's Television, Inc. v. Gen. Foods Corp., 673 P.2d 660, 668-69, 671 (Cal. 1983); Joshua D. Taylor, *Why the Increasing Role of Public Policy in California's Unfair Competition Law Is a Slippery Step in the Wrong Direction*, 52 Hastings L.J., 1131, 1133 (2001). Many argued the statute's "broad, sweeping language" was being exploited for dubious claims, becoming a cottage industry "initiated by lawyers, not injured consumers," motivated not only by the statute's broad reach but by its inclusion of the right to recover attorneys' fees for a successful action. *See, e.g.*, Cel-Tech Comms., Inc v. L.A. Cellular Tel. Co., 973 P.2d 527, 540 (Cal. 1999); Taylor, *supra*, at 1132, 1134. Mindful of "shakedown lawsuits," businesses placed proposition 64 on the California ballot in 2004, successfully amending the UCL. *See* Sharon J. Arkin, *The Unfair Competition Law After Proposition 64: Changing the Consumer Protection Landscape*, 32 W. St. U. L. Rev. 155, 167 (2005); Kevin Shelley, Sec. of the St. of Cal., Official Voter Information Guide 6 (2004).

162 *See* Cal. Bus. & Prof. Code § 17204 (West 2019); Kwikset Corp. v. Superior Court., 246 P.3d 877, 884 (Cal. 2011).

163 *See* Goonewardene v. ADP, LLC, 434 P.3d 124 (Cal. 2019).

164 Daro v. Superior Court, 61 Cal. Rptr. 3d 716, 729 (Cal. Ct. App. 2007).

165 Brown v. Electrolux Home Prods., Inc., F.3d 1125, 1235-36 (11th Cir. 2016) (citing *In re* Tobacco II Cases, 207 P.3d 20, 30 (Cal. 2009)).

166 Jenkins v. JPMorgan Chase Bank, N.A., 156 Cal. Rptr. 3d 912, 933 (Ct. App. 2013).

167 Levon Zartarian, *The Cost of Losing Money or Property for Standing in California Unfair Competition and False Advertising Lawsuits: Kwikset Corp. v. the Superior Court of Orange County*, 39 W. St. U. L. Rev. 55, 64 (2011).

168 Kwikset Corp. v. Superior Court, 246 P.3d 877, 881, 883 (Cal. 2011).

169 Hinojos v. Kohl's Corp., 718 F.3d 1098, 1105 (9th Cir. 2013).

170 *Id.* at 1104.

171 Hansen v. Newegg.com Ams., Inc., 236 Cal. Rptr. 3d 61, 67-68 (Cal. Ct. App. 2018).

172 Aishik Chakraborty et al., *Detection of Sockpuppets in Social Media*, ACM Conf. on Computer Supported Cooperative Work and Soc. Computing at 243, 243-44 (2017). "Song of the Sibyl" is an ancient Gregorian chant prophesying the apocalypse. *The Song of the Sibyl*, Wikipedia, https://en.wikipedia.org/wiki/The_Song_of_the_Sibyl [https://perma.cc/K5VY-5Y2L] (last visited Mar. 20, 2020).

173 Zhi Yang et al., *Uncovering Social Network Sybils in the Wild*, 8 ACM Transactions on Knowledge Discovery from Data 1, 3 (2014).

174 Social network accounts publicly express interest and approval with online mechanisms--for example, with a "follow," "like," "upvote," or "re-repost." *See, e.g.*, Caroline Ponessa, *Social Media 101: How to Consistently Put Out Great Content on the Big Three*, Medium: Better Marketing (Aug. 6, 2019), https://medium.com/better-marketing/social-media-marketing-101-lessons-from-a-so-called-professional-b6c99215f989 [https://perma.cc/RM2Y-UBK6].

175 A recent *New York Times* exposé revealed the actions of Devumi, a company that sold "social network amplification" through its "3.5 million automated [Twitter] accounts, each sold many times over, [totaling] more than 200 million Twitter followers." Nicholas Confessore et al., *The Follower Factory*, N.Y. Times (Jan. 27, 2018), https://www.nytimes.com/interactive/2018/01/27/technology/social-media-bots.html [https://perma.cc/RF7S-VBLW]. Its clients included known actors, professional athletes, models, a tech CEO billionaire, celebrity chefs, political pundits, and PR experts. *Id.* That was just one company. Since the article, Devumi's website accepts "no new clients," referring users to other social boosters, but many other "social amplification" sites openly advertise, able to deliver "a huge following on almost any social media platform" with "little more than a credit-card number." *See* Nicholas Confessore, *Firm that Sold Social Media Bots Settles with New York Attorney General*, N.Y. Times (Jan. 30, 2019), https://www.nytimes.com/2019/01/30/technology/letitia-james-social-media-bots.html [https://perma.cc/Z345-U8MB]; Confessore et al., *supra*. Other discreet companies like Devumi likely exist. Confessore et al., *supra*; *see also* Social Boss, socialboss.org [https://perma.cc/YKD5-3Y5Q] (last visited Mar. 27, 2020) (noting it is used for "innovative social media promotional solutions").

176 "Social commerce" is a term coined for the nexus of online sales and social networking, including websites like eBay or Etsy, where consumers act as "sellers or curators of online stores," and "social shopping," wherein consumers review products and services, influencing other fellow consumers' decisions. Catherine Baethge et al., *Social Commerce--State-of-the-Art and Future Research Directions*, 26 Electronic Mkts. 269, 270 (Aug. 2016); *see also* J. Clement, *Social Commerce Statistics & Facts*, Statista (Aug. 14, 2019), statista.com/topics/1280/social-commerce [https://perma.cc/W7UZ-6Y3E].

177 Bots can also make actual purchases posing as human buyers, increasing products' marketplace rating and visibility. *See, e.g.*, Darren Allan, *Adidas and Nike Shoes Are More Expensive Because of 'Sneaker Bots'*, TechRadar (Dec. 18, 2019), https://www.techradar.com/news/adidas-and-nike-shoes-are-more-expensive-because-of-sneaker-bots [https://perma.cc/Q9HH-LMU9].

178 John E. Dunn, *Twitter Struggles to Deal with the Sock-Puppet and Bot Armies*, Naked Security by Sophos (Sept. 1, 2017), https://nakedsecurity.sophos.com/2017/09/01/twitter-struggles-to-deal-with-the-sock-puppet-and-bot-armies/ [https://perma.cc/XUW7-U23W].

179 Dave Maass, *Four Steps Facebook Should Take to Counter Police Sock Puppets*, EFF (Apr. 14, 2019), https://www.eff.org/deeplinks/2019/04/facebook-must-take-these-four-steps-counter-police-sock-puppets [https://perma.cc/V3LR-33ZP].

180 Shareen Pathak, *Amazon Reviews Have a Bot Problem*, Digiday (Sept. 18, 2017), https://digiday.com/marketing/amazon-reviews-bot-problem/ [https://perma.cc/3J5QN4MK] (quoting Fred Killingsworth, Amazon CEO, as saying, "Amazon is this great equalizer in that competitors can come out of anywhere; bot reviews skew the experience").

181 *See* Yuanshun Yao et al., *Automated Crowdturfing Attacks and Defenses in Online Review Systems*, Conf on Computer and Comms Security, Oct. 2017, at 1143. Researchers at the University of Chicago designed an AI program that writes Amazon reviews; Amazon users thought the reviews by the AI program were real just as often as the reviews by actual human writers, especially when they offered extreme reviews (1 or 5 stars). *See id.* at 1151.

182 Kurt Thomas et al., *Trafficking Fraudulent Accounts: The Role of the Underground Market in Twitter Spam and Abuse*, Usenix Security Symp., Aug. 2013, at 195.

183 Tom Simonite, *Fake Persuaders*, MIT Tech Rev. (Mar. 23, 2015), https://www.technologyreview.com/s/535901/fake-persuaders/?set=535816) [https://perma.cc/TC87-C9MY].

184 *See* Adrien Guille et al., *Information Diffusion in Online Social Networks: A Survey*, 42 ACM SIGMOD Record 17, 19 (June 2013). This poses a legitimate issue in the commercial context. *See* Wenjing Duan et al., *Informational Cascades and Software Adoption on the Internet: An Empirical Investigation*, 33 Mgmt Info Sys. Q. 23, 23 (Mar. 2009). Researchers at the University of Rochester in New York studying the effects of information cascading on internet purchasers of software found that inferior products are often adopted simply because of the perception online that they are more popular. *Id.* "With easy availability of information about other users' choices, the Internet offers an ideal environment for informational cascades." *Id.*

185 *See* Gang Wang et al., *Serf and Turf: Crowdturfing for Fun and Profit*, Int'l World WideWeb Conf. 679, 679 (Apr. 2011).

186 Robyn Caplan & Danah Boyd Data & Soc'y Who Controls the Public Sphere in an Era of Algorithms Mediation Automation Power 6 (May 13, 2016), https://datasociety.net/pubs/ap/MediationAutomationPower_2016.pdf [https://perma.cc/8MXRS63Z] ("[A]utomated processes can be used to shift conversation quickly and swiftly, through increasing 'noise' and making it harder for

interested individuals to find relevant information, or through inserting doubt and new questions into political conversations, which posits competing views against each other.").

187 Yuanshun Yao et al Automated Crowdturfing Attacks and Defenses in Online Review Systems 1 (2017), https://people.cs.uchicago.edu/~ravenben/publications/pdf/crowdturf-ccs17.pdf [https://perma.cc/MWK3-PD7L].

188 Ebru Uzunoōlu & Sema Misci Kip, *Brand Communication Through Digital Influencers: Leveraging Blogger Engagement*, 34 Int'l J. Info Mgmt. 592 (2014).

189 Rosario Méndez, *If Influencers Are Paid, They Must Disclose It*, FTC Consumer Info. (Sept 7, 2017), https://www.consumer.ftc.gov/blog/2017/09/if-*influencersarepaidtheymustdisclose-it* [https://perma.cc/JRN9-8LLV].

190 Trial Court Order at 2, Gateway Sci. & Eng'g, Inc. v. L.A. Unified Sch., Dist., No. BC606315 (Cal. Sup. Ct. May 25, 2017), 2017 WL 3310909, at *2.

191 Indeed, many of the cases examining causation under the UCL have rejected standing only because the defendant's unfair competition lawbreaking was *entirely unrelated* to the plaintiff's injury. *See, e.g.*, Daro v. Superior Court, 61 Cal. Rptr. 3d 716 (Cal. Ct. App. 2007).

192 Engalla v. Permanent Med. Grp., Inc., 938 P.2d 903, 919 (Cal. 1997); *see also* Wennerholm v. Stanford Univ. Sch. of Med., 128 P.2d 522, 524 (Cal. 1944).

193 Adrienne LaFrance, *The Internet Is Mostly Bots,* Atlantic (Jan. 31, 2017), https://www.theatlantic.com/technology/archive/2017/01/bots-bots-bots/515043/ [https://perma.cc/ZQ64-M5YD].

194 Alliance Mortg. Co. v. Rothwell, 900 P.2d 601, 609 (Cal. 1995).

195 CACI No. 1908., *Reasonable Reliance, in* Judicial Council of California Civil Jury Instructions 1099, 1099 (2017).

196 Seeger v. Odell 115 P.2d 977, 980-81 (Cal. 1941).

197 *Why Are Seniors the Fastest-Growing Demographic on Social Media?*, NPR (Nov. 25, 2013, 4:31 PM), https://www.npr.org/templates/story/story.php?storyId=247220424 [https://perma.cc/AM4Y-PF47].

198 This Author is a Generation Xer and does not have a dog in this fight.

199 Stansfield v. Starkey, 267 Cal. Rptr. 337, 339 (Cal. Ct. App. 1990).

200 Bigler-Engler v. Breg, Inc., 213 Cal. Rptr. 3d 82, 103 (Cal. Ct. App. 2017).

201 Online, "butthurt" means childish resentment after public punishment (like a child who has been spanked) and is often hurled at online commenters who cannot admit their claim or reasoning has been credibly disproven. *See* Aesop's Fables 23 (V.S. Vernon Jones trans., Wordsworth Editions Ltd. 1994) (describing the story of "sour grapes").

202 *See* Cal Bus. & Prof Code § 17203 (West 2019).

203 S*ee* Bank of the West v. Superior Court, 833 P.2d 545, 553 (Cal. 1992).

204 Kwikset Corp. v. Superior Court, 246 P.3d 877, 890 (Cal. 2011).

205 *Id.* at 889.

206 Hansen v. Newegg.com Ams., Inc., 236 Cal. Rptr. 3d 61, 67, 72 (Cal. Ct. App. 2018) (*"Kwikset* makes clear that Proposition 64 was not intended to eliminate consumers' ability to pursue UCL ... claims for misleading advertisements that induced them to make a purchase they would not have otherwise made.").

207 *See* People v. Overstock.com, Inc., 219 Cal. Rptr. 3d 65, 76, 87 (Cal. Ct. App. 2017). (dealing with a UCL action by a public prosecutor against an online vendor advertising nonexistent drops in price).

208 *See* Kimberly A. Kralowec, Kralowec Law, P.C., The UCL Practitioner, https://www.uclpractitioner.com/ [https://perma.cc/PJ9B-QC8N] (consumer legal practice resource).

209 Standing requirements apply to class actions, but an ongoing debate of conflicting court opinions exists on the subject of whether the "injury-in-fact" proof applies only to the lead plaintiff or to all potential class plaintiffs. Such questions lie beyond the scope of this Article, especially since March 2019, when the Supreme Court issued a per curiam opinion in the settlement of a class-action case against Google for violating privacy laws, vacating the decision and sending the case back to the Ninth Circuit for reconsideration of Article III standing issues. *See* Frank v. Gaos, 139 S. Ct. 1041, 1046 (2019).

210 The biggest challenge to a class action enforcing the CA Bot Act is likely the plaintiff's burden of showing a class is *ascertainable*, a function of a number of factors, including "the probability each member [of the proposed class] will come forward ultimately, identify himself, and prove his separate claim to a portion of the total recovery. Noel v. Thrifty Payless, Inc., 226 Cal. Rptr. 3d 465, 472 (Cal. Ct. App. 2017). The unanswered question right now in California class-action jurisprudence is whether the plaintiff is required to identify with specificity records in existence to identify the class already exists, as ruled in 2017 by the California appellate court in *Noel*. In denying the class, the court cited the plaintiff's lack of significant evidence showing how the class would be ascertained, departing from an older approach requiring only an allegation that the defendant's records will contain information needed to ascertain the members of an existing class. *Compare Noel*, 226 Cal. Rptr. 3d at 472, *with* Daar v. Yellow Cab Co., 67 Cal.2d 695 (1967). This ruling in *Noel* is at odds with *Daar v. Yellow Cab Co.* The California Supreme Court has taken up the issue, but until it provides greater clarity, a complaint should at least allege with particularity the methods and records available to identify class members and "how burdensome their production would be." Expert testimony, or at least a reasonable grasp of the forensic methods, in identifying anonymous online users would be beneficial in drafting a complaint.

211 Christina Ng, *Crime Writer RJ Ellory Caught Faking Amazon Reviews*, ABC News (Sept. 3, 2012), https://abcnews.go.com/International/crime-writer-rj-ellory-caught-faking-amazon-reviews/story?id=17143005 [https://perma.cc/FRT8-QHEX]. Crime-fiction writer RJ Ellory had an assumed Amazon account writing reviews praising his books and slamming his competitors; given the importance of such reviews to sellers, and the alleged prevalence of such fake reviews, potential defendants may exist. *Id.*

212 *See* Abdullah Mueen et al., Presentation at the University of New Mexico Department of Computer Science's Conference on Information and Knowledge: Taming Social Bots: Detection, Exploration and Measurement, (Nov. 2019), https://www.cs.unm.edu/~mueen/Tutorial/TamingBots.html [https://perma.cc/2EHQ-UG4A].

213 *See, e.g.*, Ethan Wolff-Mann, *People Are Beating Equifax in Appeals Court and Winning Thousands*, Yahoo Fin. (Mar. 9, 2018), https://finance.yahoo.com/news/people-beating-equifax-appeals-court-winning-thousands-210943746.html [https://perma.cc/QMD8-J6RZ] (describing a class action brought against credit reporting agency Equifax that has recovered thousands of dollars for plaintiffs).

214 Uzunoōlu & Kip, *supra* note 188.

215 Siyoung Chung & Hichang Cho, *Fostering Parasocial Relationships with Celebrities on Social Media: Implications for Celebrity Endorsement*, 34 Pysch. & Marketing 481, 481 (Apr. 2017).

216 Cel-Tech Commc'ns v. L.A. Cellular Tel. Co., 973 P.2d 527, 544 (Cal. 1999). The court also stated unfairness in competitor actions might require antitrust behavior. But courts have held that commercial deceit can violate antitrust laws where intent and other fraud elements are present, as in the CA Bot Act. *See, e.g.*, Note, *Deception as an Antitrust Violation*, 125 Harv. L. Rev. 1235, 1236 (Mar. 2012).

217 *Cel-Tech Commc'ns*, 973 P.2d at 544.

218 People *ex rel.* Mosk v. National Research Co., 20 Cal. Rptr. 516, 521 (Cal. Ct. App. 1962); Kasky v. Nike, Inc., 45 P.3d 243, 249 (Cal. 2002); *Cel-Tech Commc'ns*, 973 P.2d at 544; Am. Philatelic Soc. v. Claibourne, 46 P.2d 135, 140 (Cal. 1935).

219 *See, e.g., New Trend of Product Review Manipulation Single Review Buyer Accounts (Probably Bots)*, Amazon Seller Fs. (July 2019), https://sellercentral.amazon.com/forums/t/new-trend-of-product-review-manipulation-single-review-buyer-accounts-probably-bots/478940 [https://perma.cc/Y527-TTCA].

220 *Compare* Glen Oaks Estates Homeowners Assn. v. Re/Max Premier Props., Inc., 137 Cal. Rprt. 3d. 865, 871 (Cal. Ct. App. 2012) (citing Stearman v. Centex Homes 92 Cal. Rprt. 2d 761, 771 (Cal. Ct. App. 2000) (permitting expert-witness fees in preparing a UCL action constituted injury in fact)), *with* Two Jinn, Inc. v. Gov't Payment Serv., Inc., 183 Cal. Rptr. 3d 432, 442 (Cal. Ct. App. 2015) ("'[P]re-litigation costs' do not establish standing [in] a UCL claim because they are not caused by the business practices ... [characterized] as unlawful.").

221 *See, e.g.*, Engalla v. Permanente Med. Grp., Inc., 938 P.2d 903, 917 (Cal. 1997) (quoting Lazar v. Superior Court, 909 P.2d 981, 985 (Cal. 1996)) ("An action for promissory fraud may lie where a defendant fraudulently induces the plaintiff to enter into a contract.").

222 *See Lazar*, 909 P.2d at 985.

223 *CACI No. 3905A, Physical Pain, Mental Suffering, and Emotional Distress (Noneconomic Damage), in* Judicial Council of California Civil Jury Instructions 756, 757 (2017).

224 Plotnik v. Meihaus, 146 Cal. Rptr. 3d 585, 596 (Cal. Ct. App. 2012).

225 Janna Anderson & Lee Rainie, *The Future of Truth and Misinformation Online*, Pew Res Ctr. (Oct. 19, 2017), https://www.pewresearch.org/internet/2017/10/19/the-future-of-truth-and-misinformation-online/ [https://perma.cc/A93M-SJ7J].

226 David A. Broniatowski et al., *Weaponized Health Communication: Twitter Bots and Russian Trolls Amplify the Vaccine Debate*, 108 Am. J. Pub Health 1378, 1378 (May 22, 2018) (concerning the debate over mandatory vaccination).

227 *See, e.g.*, Anna Kata, *A Postmodern Pandora's Box: Anti-vaccination Misinformation on the Internet*, 28 Vaccine 1709, 1709 (2010).

228 *See, e.g.*, Cal Health & Safety Code § 42400(d) (West 2018) (governing air pollution harm and stating that an actual injury is one that "in the opinion of a licensed physician and surgeon, requires medical treatment involving more than a physical examination").

229 *See Reliance, Causation and Injury in Business and Professions Code Section 17200 and 17500 Cases After Proposition 64*, Robins Kaplan LLP (Sept. 10, 2008), https://www.robinskaplan.com/resources/publications/2008/09/reliance-causation-and-injury-in-business-and-professions-code-section-17200-and-17500-cases-after__ [https://perma.cc/MN9QFG54]; Steve Boranian, *A Money-For-Nothing Pharmaceutical Class Action in California*, Drug & Device L. Blog (July 12, 2019), https://www.druganddevicelawblog.com/2019/07/a-money-for-nothing-pharmaceutical-class-action-in-california.html [https://perma.cc/5JKP-3YV6].

230 *See, e.g.*, In re Tobacco II Cases, 207 P.3d 20, 40 (Cal. 2009); Jackson v. California Dept. of Corrections & Rehabilitation, No. F072573, 2017 WL 168863, at *4 (Cal. Ct. App. 2017) (concerning a prison inmate's health problems allegedly caused by drinking water that authorities represented was potable).

231 Howard Rheingold The Virtual Community Homesteading on the Electronic Frontier 103 (1993).

232 *Id.* at 190-91.

233 *Id.*

234 Emilio Ferrara, *Disinformation and Social Bot Operations in the Run up to the 2017 French Presidential Election*, U.S.C. Info Sci Inst. (July 2017), https://arxiv.org/pdf/1707.00086.pdf [https://perma.cc/LG8K-55X2] ("[U]sage patterns suggest ... existence of a black-market for political disinformation bots.").

235 Norah Abokhodair et al., *Dissecting a Social Botnet: Growth, Content and Influence in Twitter*, ACM Conf on Computer-Supported Cooperative Work & Soc Computing (Feb. 2015), https://arxiv.org/pdf/1604.03627.pdf [https://perma.cc/GAY5-HQU4].

236 Rod J. Rosenstein, U.S. Dep't of Justice Report of the Attorney General's Cyber Digital Task Force 2 (July 2, 2018).

237 Report of the Select Committee on Intelligence on Russian ActiveMeasures Campaigns and Interference in the 2016 U.S. Election Volume 2: Russia's Use of Social Media with Additional Views, S. Rep. No. 116-XX at 1 (2019).

238 Christopher A. Bail et al., *Exposure to Opposing Views on Social Media Can Increase Political Polarization*, 115 Proc Nat'l Acad Sci. U.S. 9216, 9216 (Aug. 28, 2018).

239 *Id.*

240 Alice E. Marwick & Ross Miller, *Online Harassment, Defamation, and Hateful Speech: A Primer of the Legal Landscape*, Fordham Ctr. L. & Info Policy 1, 7 (June 10, 2014). The CA Bot Act excludes from liability ISPs, OSNs, or publications with "10,000,000 or more unique monthly U.S. visitors or users for a majority of months" in a year. *See* Cal Bus. & Prof. Code §§ 17940(c), 17942(c) (West 2019). Smaller providers of social networking apps or websites might be vicariously liable for hosting nondisclosing bot activity, like fake online reviews or endorsements, if they are warned and fail to police it. But even smaller providers likely may have a potential defense in section 230 of the 1996 Communications Decency Act (CDA), intended as a safe harbor for ISPs and content hosts by providing that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." 47 U.S.C. § 230(c)(1) (2018). Section 230 has been applied unevenly, with liability occasionally imposed in certain failure-to-warn cases with highly sympathetic plaintiffs. *See* Eric Goldman, *Section 230 Baffles 9th Circuit (Again)*-Doe #14 v. ModelMayhem, Tech. & Marketing L. Blog (May 31, 2016), https://blog.ericgoldman.org/archives/2016/05/section-230-baffles-9th-circuit-again-doe-14-v-modelmayhem.htm [https://perma.cc/5664-4R3E]. But the California Supreme Court confirmed section 230's broad immunity in its closely watched 2017 opinion in *Hassell v. Bird*, involving defamatory statements made by a defendant on the collaborative review website Yelp. Hassell v. Bird, 420 P.3d 776, 793 (Cal. 2018). The California Supreme Court has even extended section 230 of the CDA to include an individual user defendant who reposted defamatory statements by other users about the plaintiff. Barrett v. Rosenthal, 150 P.3d 510, 529 (Cal. 2006).

241 Victoria L. Rubin et al., *Deception Detection for News: Three Types of Fakes*, 52 Proc. Assoc Info Sci. & Tech. 1 (Feb. 24, 2016).

242 For example, Facebook has been accused of both harboring anti-conservative bias and permitting pro-conservative fake news.

243 Xinyi Zhou & Reza Zafarani, Fake News: A Survey of Research, Detection Methods, and Opportunities (Dec. 2, 2018) (unpublished manuscript), https://arxiv.org/pdf/1812.00315.pdf [https://perma.cc/YF8J-XV9V].

244 *See, e.g.*, Claire Wardle & Hossein Derakhshan, *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*, Council Eur. 1, 12 (Sept. 27, 2017), https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c [https://perma.cc/SG85-SU9S]; Jane Coaston, *The Facebook Free Speech Battle, Explained*, Vox (May 14, 2019), https://www.vox.com/technology/2019/5/6/18528250/facebook-speech-conservatives-trump-platform-publisher [https://perma.cc/3EH2-K9NG]; Andrew Hutchinson, *Facebook Announces Bans of Well-Known Extremist Commentators*, Soc Media Today (May 3, 2019), https://www.socialmediatoday.com/news/facebook-announces-bans-of-well-known-extremist-commentators/553989/ [https://perma.cc/R6RF-UCX8].

245 *See* Cal Bus. & Prof Code § 17491(a) (West 2019). The law requires disclosure of deceptive bots communicating with people online to "influence a vote."

246 Cal Senate JudiciaryComm Senate Bill 1001 Analysis, 2017-2018 Regular Sess. (Apr. 23, 2018).

247 Rod J. Rosenstein, Deputy Att'y Gen., *Report of the Attorney General's Cyber Digital Task Force*, U.S. Dep't Just. (July 2, 2018).

248 *See, e.g.*, Nixon v. Herndon, 273 U.S. 536 (1927) (concerning a Texas Democratic Party rule that banned African American members or candidates).

249 42 U.S.C. § 1985 (2018) ("[I]f two or more persons conspire to prevent by force, intimidation, or threat, any citizen who is lawfully entitled to vote, from giving his support or advocacy in a legal manner, toward or in favor of [a federal] election the party so injured or deprived may have an action for the recovery of damages against the conspirators.").

250 *See* Cal Gov't Code § 84504 (West 2018).

251 Memphis Comm. Sch. Dist. v. Stachura, 477 U.S. 299, 301-02 (1986); Jean C. Love, *Presumed General Compensatory Damages in Constitutional Tort Litigation: A Corrective Justice Perspective*, 49 Wash. & Lee L. Rev. 67, 80 (1992); *see* Carey v. Piphus, 435 U.S. 247, 254 (1978).

252 Love, *supra* note 252, at 80; *see Piphus*, 435 U.S. at 254; *Stachura*, 477 U.S. at 301-02.

253 *See, e.g.*, United States v. Alvarez, 567 U.S. 709, 709 (2012). The Supreme Court set aside the conviction of an elected representative of the water board who offered false military accomplishments while presiding at a water board meeting under the federal Stolen Valor Act, which outlawed false claims of military accomplishments and medal receipt. *See id.* The Stolen Valor Act was effectively struck down. *See id.*

254 *See* Deceptive Practices and Voter Intimidation Prevention Act of 2018, S. 3279 115 Cong. (2017-2018).

255 *See* Earl Bousquet, *Caribbean Elections in the Age of Cambridge Analytica: SCL, Cambridge Analytica's Caribbean History*, Cayman Islands iNews (July 29, 2018), https://www.ieyenews.com/caribbean-elections-in-the-age-of-cambridge-analytica-scl-cambridge-analyticas-caribbean-history/ [https://perma.cc/B75F-45L9]; Paul Hilder, *'They Were Planning on Stealing the Election': Explosive New Tapes Reveal Cambridge Analytica CEO's Boasts of Voter Suppression, Manipulation and Bribery*, Open Democracy (Jan. 2019), https://www.opendemocracy.net/en/dark-money-investigations/they-were-planning-on-stealing-election-explosive-new-tapes-reveal-cambridg/ [https://perma.cc/UK8Q-MK2W]; Jada Steuart, *Netflix's 'The Great Hack' Highlights Cambridge Analytica's Role in Trinidad & Tobago Elections*, Global Voices AdVox (Aug. 6, 2019), https://advox.globalvoices.org/2019/08/06/netflixs-the-great-hack-highlights-cambridge-analyticas-role-in-trinidad-tobago-elections/ [https://perma.cc/USS7-FBYK]. For example, Cambridge Analytica's parent company worked in Trinidad and Tobago; CEO Alexander Nix claimed the company successfully engineered a grassroots social media campaign to "increase apathy" and discourage young Afro-Caribbeans from voting. Its client won. Hilder, *supra*; Steuart, *supra*.

256 *See* Christopher Bing, *Exclusive: Twitter Deletes over 10,000 Accounts that Sought to Discourage U.S. Voting*, Reuters (Nov. 2, 2018), https://www.reuters.com/article/us-usa-electiont-witter-exclusive/exclusive-twitter-deletes-over-10000-accounts-that-sought-to-discourage-u-s-voting-idUSKCN1N72FA [https://perma.cc/7MFS-Q8T7].

257 Cal Bus. & Prof Code § 17203 (West 2019).

258 *See, e.g.*, Kwan v. Mercedes-Benz of North Am., Inc., 28 Cal. Rptr. 2d 371, 371 (1994).

259 *See* Cal Civ Code § 1750 et seq. (West 2019). Deceptive bot speech might be considered misrepresenting an association with another, disparaging the goods of another by false or misleading representation of facts, or omitting a material fact in the sale of goods to a consumer. *Id.* If the defendant knows the truth, failing to disclose is "misleading in light of other facts that [the defendant] did disclose." *See also* Bank of the West v. Superior Court, 833 P.2d 545 (Cal. 1992); Gutierrez v. Carmax Auto Superstores Cal., 248 Cal. Rptr. 3d 61 (Cal. Ct. App. 2018).

260 *See, e.g.*, Robinson Helicopter Co. v. Dana Corp., 102 P.3d 268, 272 (Cal. 2004); Hunter v. Up-Right, Inc., 864 P.2d 88, 90 (Cal. 1993).

261 *See* Baraniuk, *supra* note 11 ("[B]ots appeared en masse to harass [those] favoring Catalonia's referendum on independence from Spain.").

262 Zeran v. Am. Online, Inc., 129 F.3d 327 (4th Cir. 1997). Defendant-ISP AOL was held to be immune under section 230 for publishing defamatory statements and personal details of the plaintiff resulting in harassment and death threats. For daring readers, see also 4Chan, 4chan.org (last visited April 12, 2020).

263 "Swatting" raises the stakes of the traditional "bomb threat," disrupting emergency resources while focusing its harm on a particular individual or group, and has resulted in real-world violence and fatality. The notorious "Wichita swatting" involved cyberfraud to obtain victims' personal information. After the House passed a bipartisan bill to punish the practice, the bill's sponsor was subsequently swatted. *See* Joshua Miller, *Police Swarm Katherine Clark's Home After Apparent Hoax*, Bos Globe (Feb. 1, 2016), https://www.bostonglobe.com/metro/2016/02/01/cops-swarm-rep-katherine-clark-melrose-home-after-apparenthoax/yqEpcpWmKtN6bOOAj8FZXJ/story.html [https://perma.cc/KQ3T-PUX2]; *see also* Nicolas Estano, *La Criminologie de L'information: État des Lieux et Perspectives*, 52 Criminologie 13, 13-32 (2019) (The "intimacy of social media" lets a "swatting" perpetrator use bots to "recover a large amount of data [about a] future victim.").

264 This is termed "exemplary damages" in California.

265 Information can be falsified through spoofing, but it is difficult to hide an online origin from coordinated law enforcement.

266 *See* Paul Alan Levy, *Developments in Dendrite*, 14 Fla Coastal L. Rev. 1, 1 (2012). Most websites require emails for a subscription now, and the email confirmation creates a record that is difficult to hide, even by technical means.

267 *See* Harlan Yu, *The Traceability of an Anonymous Online Comment*, Freedom to Tinker (Feb. 10, 2010), https://freedom-to-tinker.com/2010/02/10/traceability-anonymous-online-comment/ [https://perma.cc/ZQS4-9LFW] ("[T]he nearly simultaneous connections to third party services means that the results of tracing can be combined.").

268 *See, e.g.*, Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146 (C.D. Cal. 2002). The defendant operated an online "age-verification system" (AVS), which confirmed online customers' age so they could access affiliated adult websites. The AVS was held liable for the copyright infringement of certain affiliated websites, despite the AVS publishing no online images and having an official policy that would ban affiliates infringing copyrights. The plaintiff had even failed to notify the defendant directly about the infringement in question, but knowledge of it was imputed to the AVS defendant because of unrelated complaints by other affiliates.

269 Hassell v. Bird, 203 Cal. Rptr. 3d 203, 224 (Cal. Ct. App. 2016) ("[Section] 230 has been construed broadly to immunize 'providers of interactive computer services against liability arising from content created by third parties.'").

270 A motion to quash asks the judge to set aside an action like a subpoena. *See Quash Law and Legal Definition*, USLegal, https://definitions.uslegal.com/q/quash/ [https://perma.cc/JE8P-PXWT] (last visited Apr. 9, 2020).

271 *See* Glassdoor, Inc. v. Superior Court of Santa Clara Cty., 215 Cal. Rptr. 3d 395, 401 (Cal. Ct. App. 2017) ("[A] substantial preponderance of national authority favors the rule that [online] publishers are entitled to assert [free speech] interests of their anonymous contributors in maintaining anonymity.").

272 *See, e.g.*, Margot E. Kamimski, *Authorship, Disrupted: AI Authors in Copyright and First Amendment Law*, 51 U.C. Davis L. Rev 589 (2017).

273 *See* Lorillard Tobacco Co. v. Reilly, 533 U.S. 525, 553-54 (2001).

274 *See* Cal Bus. & Prof Code § 17941(b) (West 2019). The provisions of this chapter are severable. If any provision of this chapter or its application is held invalid, that invalidity shall not affect other provisions or applications that can be given effect without the invalid provision or application.

275 *Compare* Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y., 447 U.S. 557 (1980) (applying strict scrutiny for commercial-speech claims), *with* Zauderer v. Office of Disc. Counsel, 471 U.S. 636 (1985) (applying rational basis for commercial-speech claims). After scholarly appeals for clarity, it seems that *Zauderer* is the applicable standard. *See* Nat'l Inst. of Family & Life Advocates v. Becerra, 138 S. Ct. 2361, 2367 (2018); Am. Beverage Ass'n v. City & Cty of S.F., 916 F.3d 749 (9th Cir. 2019).

276 *See* Kasky v. Nike, Inc., 45 P.3d 243, 303 (Cal. 2002) ("The UCL's purpose is to protect both consumers and competitors by promoting fair competition in commercial markets for goods and services.").

277 *See* Meese v. Keene, 481 U.S. 465, 481 (1987).

278 By contrast, in other cases the compelled commercial disclosures' *content* were controversial. *See, e.g., Am. Beverage Ass'n*, 916 F.3d at 749 (concerning the factual claim that sweetened beverages degrade one's health); *Becerra*, 138 S. Ct. at 2367 (concerning the claim that abortion is a valid alternative to pregnancy).

279 *Becerra*, 138 S. Ct. at 2367 (quoting *Zauderer*, 471 U.S. at 651).

280 *See* NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 462 (1958).

281 *See, e.g.*, Allison Hayward, *Anonymous Speech*, First Amend Encyclopedia (June 2017), https://www.mtsu.edu/first-amendment/article/32/anonymous-speech [https://perma.cc/BT6E-N24Q].

282 *See* Matthew J. Franck, *Should Pseudonymous Bloggers Be Outed?*, Nat'l Rev. (June 8, 2009), https://www.nationalreview.com/bench-memos/should-pseudonymous-bloggers-be-outed-matthew-j-franck/ [https://perma.cc/54KN-2H79].

283 *See* Mark D. Nozette, *Constitutional Law-First Amendment-Loyalty Oaths-Vagueness Standard Relaxed for Affirmative Oaths*, 58 Cornell L. Rev. 383, 393 (1973).

284 Kolender v. Lawson, 461 U.S. 352, 357 (1983) ("[P]enal statute [s] must define the criminal offense with sufficient definiteness that ordinary people can understand what conduct is prohibited and in a manner that does not encourage arbitrary and discriminatory treatment.").

285 *See, e.g.*, Cal Civ Pro Code § 425.16 (West 2019). "SLAPP" stands for "strategic lawsuit against public participation."

286 *See, e.g.*, cyberSLAPP.org, http://www.cyberslapp.org [https://perma.cc/JF4W-V9N4] (last visited Mar. 20, 2020).

287 *See* Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573, 577 (N.D. Cal. 1999).

288 Indep. Newspapers, Inc. v. Brodie, 966 A.2d 432, 453 (Md. 2009) (denying a subpoena to unmask anonymous defendants, citing US Supreme Court rulings recognizing a right under the First Amendment to speak anonymously).

289 *See* Highfields Capital Mgmt. v. Doe, 385 F.Supp.2d 969, 970-71 (N.D. Cal. 2005) (holding that evidence the defendant's wrongful conduct caused real harm entitled the plaintiff to conduct discovery to learn the identity of defendant by subpoena of ISP) (citing *Seescandy*, 185 F.R.D. at 580).

290 *See* Doe v. Cahill, 884 A.2d 451, 463 (Del. 2005).

291 *See* Krinsky v. Doe 6, 72 Cal. Rptr. 3d 231, 234-35 (Cal Ct. App. 2008). The court concluded the defendant's speech was opinion and not prima facie evidence of defamation and thus quashed the subpoena of Doe defendant's personal information. *Id.*

292 *See, e.g.*, John Doe No. 1 v. Reed, 561 U.S. 186, 187 (2010) (holding that referendum petitioners were required to disclose their identities).

293 *See* Glassdoor, Inc. v. Superior Court of Santa Clara Cty., 215 Cal. Rptr. 3d 395, 400 (Cal. Ct. App. 2017).

294 *See* United States v. Glassdoor, Inc., 875 F.3d 1179, 1181-82 (9th Cir. 2017).

295 *See* Lamo & Calo, *supra* note 19.

296 *See* Confessore, *supra* note 175 ("A spokeswoman said that [an] employee had acted without [fashion model Kathy] Ireland's authorization [in securing fake followers on her account] and had been suspended" after the *Times'* inquiry).

297 *See* Aaron Smith et al., *Bots in the Twittersphere*, Pew Res Ctr. (Apr. 9, 2018), https://www.pewresearch.org/internet/2018/04/09/bots-in-the-twitter-sphere/ [https://perma.cc/SBP4-PZM2] ("An estimated two-thirds of tweeted links to popular websites are posted by [bots,] not human beings.").

298 Ryan Erskine, *You Just Got Attacked By Fake 1-Star Reviews. Now What?*, Forbes (May 15, 2018), https://www.forbes.com/sites/ryanerskine/2018/05/15/you-just-got-attacked-by-fake-1-star-reviews-now-what/ [https://perma.cc/YMZ4-LLXY].

299 Online bots post about porn, sports, and commercial products more than politics. *See* Smith et al., *supra* note 297.

300 Adrian Shahbaz, *Freedom on the Net 2018: The Rise of Digital Authoritarianism*, Freedom House (2018), https://freedomhouse.org/report/freedom-net/freedom-net-2018/rise-digital-authoritarianism [https://perma.cc/YQ35-QCCV] (internal quotations removed).

301 *See* Emilio Ferrara et al., *Bots Increase Exposure to Negative and Inflammatory Content in Online Social Systems*, 115 PNAS 12435, 12439-40 (2018).

302 *See* Baraniuk, *supra* note 11 ("Bots appeared en masse to harass [those] favoring Catalonia's referendum on independence from Spain.").

303 Bots have been active in political elections in Kenya, Rwanda, Angola, Egypt, Lesotho, Senegal, and Equatorial Guinea. Abdi Latif Dahir, *How Social Media Bots Became an Influential Force in Africa's Elections*, Quartz Afr. (July 18, 2018), https://qz.com/africa/1330494/twitter-bots-in-kenya-lesotho-senegal-equatorial-guinea-elections/ [https://perma.cc/5N6T-PF7W].

304 *See* Fabian Schäfer, Philipp Heinrich & Stefan Evert, *Japan's 2014 General Election: Political Bots, Right-Wing Internet Activism, and Prime Minister Shinzō Abe's Hidden Nationalist Agenda*, 5 Big Data 294, 294-309 (Dec. 1, 2017), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5733662/ [https://perma.cc/76AJ-Q5MQ]. Bots aided nationalist online support for Shinzo Abe.

305 *See* Allie Funk, *Asia's Elections Are Plagued by Online Disinformation*, Freedom House (May 2, 2019), https://freedomhouse.org/article/asias-elections-are-plagued-online-disinformation [https://perma.cc/AYJ2-CB6F].

306 *See* Chris Roper, *American Fake Twitter Accounts Boost Messaging as ANC Picks New Leader*, Medium (Dec. 21, 2017), https://medium.com/code-for-africa/american-fake-twitter-accounts-boost-messaging-as-anc-picks-new-leader-5414f28ab5d0 [https://perma.cc/4D9Z-DVWT].

307 *See* Andrew Allen, *Bots in Brazil: The Activity of Social Media Bots in Brazilian Elections*, Wilson Ctr. (Aug. 17, 2018), https://www.wilsoncenter.org/blog-post/bots-brazil-the-activity-social-media-bots-brazilian-elections [https://perma.cc/UU7K-KE8G].

308 *See* Ben Collins & Shoshana Wodinsky, *Twitter Pulls Down Bot Network that Pushed Pro-Saudi Talking Points About Disappeared Journalist*, NBC News (Oct. 18, 2018), https://www.nbcnews.com/tech/tech-news/exclusive-twitter-pulls-down-bot-network-pushing-prosaudi-talking-n921871 [https://perma.cc/E74J-D7U6].

309 *See* Tom Rasmussen, *There Was a Tinder Election Bot Fanning the Fire of the Youth*, i-D (June 15, 2017), https://i-d.vice.com/en_uk/article/3kd87w/general-election-tinder-bot-youth-vote [https://perma.cc/7MMP-BKHS].

310 Senate Judiciary Committee, *supra* note 12, at 9.