Cameron Irby

Dr. Knight

ATCM 6300

11 December 2018

From Clowns to Google Bombs: The Evolution of Digital Hate

With the constant news updates about how our private information has been hacked from (insert large corporation here), we've come to just accept it as part of the norm; it's all online, so it doesn't affect us in reality. But this kind of technological optimism has blinded many to what we already know. We ignore the one or two angry messages sent our way from names we don't recognize. We view the vitriol in our News Feeds as a glitch in Facebook's algorithms that'll get patched out eventually. If any negative attention turns our way, common wisdom is to just stay offline for a while and wait it out. In the wake of the #MeToo movement, Gamergate, and an ever-growing body of evidence, to say that we can be safe on the Internet or just disconnect is naïve at best. But at its worst, such a sentiment is dangerous to hold. So, too, is the idea that all these reports of toxic behavior on the Internet are a recent phenomenon. As evidenced by Julian Dibbell's account of how the LambdaMOO community struggled to address a clear instance of cyber rape as well as the continued debate over hate speech on social media, the threat of misogynist, racist, and hateful acts ingrained itself to the Internet early on, and the increased demand for a personalized Web serves only to grant malcontents with more ammunition to drive us off of the face of the Internet.

However, I must begin this essay with a few hard truths. First, I (a white male with little social media presence who tends to keep political/social opinions private or, at least, offline)

have experienced some harassment online, but nothing that I have encountered in my life could begin to compare to the torment that women, people of color, and those who wear their alternate sexual orientations and relationships openly face on a daily basis. The group Working to Halt Online Abuse (WHOA) found that over 70% of online harassment victims are female compared to roughly 20% of men and 5% unknown-and another study found 33% of LGBT students at the University of New Hampshire received hate-laced messages and death threats (qtd in Citron 13, 15). And while white, cisgender, straight males can also become victims, they are often spun by their attackers as being gay, a woman in disguise, a religious minority, or a sex offender; in other cases, threats are made against women in their lives (wives, daughters, sisters, etc.), a stab that could be even more psychologically damaging than if it was aimed at the target himself (Citron 15, Jane 11). Nevertheless, the majority of online hate crimes match up with their real-world counterparts; misogyny, racism, and homo/transphobia will be found online as long as people are misogynist, racist, and homo/transphobic in general. To appear neutral and state that toxicity affects everyone equally would only contribute to the dilution of any discussion of this topic.

The other major disclaimer I must make about this essay is that the language of harassment will make readers uncomfortable. For the harassers, that is entirely the point: to make their intended recipient feel as disgusted and unsafe as possible. We cannot simply tidy up the vitriolic tweets to make them consumable for a wider audience; per Emma Jane in *Misogyny Online*, "Regardless of individual researchers' tastes and tolerance for material outside their comfort zones, when academics cite only the tamest examples or rely on euphemisms, they inadvertently position online hostility as a mild and mostly benign practice," which allows us plausible deniability in that the problem doesn't *seem* so bad (104). If by exposing the infernal

language of trolls, harassers, and misogynists I am considered unprofessional, then perhaps we should reconsider what "professionalism" is. Witnessing the suddenness, crudeness, and vile nature of online harassment and toxic behavior will be painful, both to those who've never faced harassment and to anyone who has ever found hate mail in their inbox, been the center of an online riot, or faced the systemic issues keeping them from speaking up. If we cannot face reality, we cannot change it.

Part of the reason why people don't tell others about the harassment they have received is because often nothing comes of it. Danielle Citron, author of *Hate Crimes in Cyberspace*, writes that in most cases, victims don't talk to the police because they won't act on it (20). The abuse that is hurled at us online is not only morally reprehensible but in many cases, illegal, yet, Citron continues, police around the world are woefully ignorant of the technical knowledge required to locate perpetrators and assume that victims can just "log out" for a while and be fine (20). This imagined barrier between what happens on the Web and what happens in reality provides a convenient out for those who want to ignore the problem and hope it goes away on its own. However, this excuse allows abusers the same levity; if a woman doesn't like getting unsolicited dick pics on Snapchat, they might say, then she shouldn't use Snapchat. Not only does this sentiment blame the victim for stepping out into the digital sphere, but it also blatantly ignores how hate online can have significant effects offline.

Take, for instance, LambdaMOO. Founded by Pavel Curtis at Xerox PARC in 1991, LambdaMOO was an offshoot of the popular Multi-User Dungeons (MUDs) that allowed participants to play *Dungeons & Dragons*-esque role-playing games online. The MUD format was tweaked later on to allow each interactor the ability to create their own objects within the game and define that object's properties, leading to the acronym MOO (MUD, object-oriented). LambdaMOO (or Lambda) began as a side project. Per Curtis, "To a large degree, I was in it for the technology. I thought it was just cool to have this language and this ability to make things intelligent or interesting artifacts that people could play with, and it was just this great playground, and I was just assuming that everybody would be happy to be there" (qtd. in Laurel 116). The layout of LambdaMOO was based on Curtis's home, with guests entering via a portal in a virtual coat closet and choosing how they wished to be represented. As players had the ability to manipulate just about anything in the game they could choose whatever appearance they desired, craft additional rooms in the Lambda mansion, use alternative pronouns, and do whatever they liked.

In March of 1993, someone decided that they would like to rape people in LambdaMOO. Dibbell describes "Mr. Bungle" as "a fat, oleaginous, Bisquick-faced clown dressed in cumstained harlequin garb and girdled with a mistletoe-and-hemlock belt whose buckle bore the quaint inscription "*KISS ME UNDER THIS, BITCH!*" (239, original emphasis). Mr. Bungle had taken advantage of LambdaMOO's object creation and found out that he could force people to act against their will. And so, Mr. Bungle created a voodoo doll and forced "legba, a Haitian trickster spirit of indeterminate gender, brown-skinned and wearing an expensive pearl-grey suit" to "sexually service him in a variety of more or less conventional ways" (239). He then proceeded to use the doll on a female character, Starsinger, to make her commit acts with other people in the room and "violate herself with a piece of kitchen cutlery" (240). Hundreds of other guests in the mansion bore witness to this event, but none had the power to actually stop him. They needed a wizard, otherwise known as an administrator.

Once Mr. Bungle was caged by a wizard (and then promptly let out by someone who didn't notice what happened), the members of LambdaMOO convened to discuss the aftermath.

legba and Starsinger wanted Mr. Bungle "toaded"—a permanent ban that would not only destroy any virtual presence of the individual but also prevent their IP address from being registered to another account and something that only a wizard could do. And while a wizard could do so on their own terms for whatever reason, Curtis had recently set up new rules for LambdaMOO stating that "the wizards…were pure technicians. From then on, they would make no decisions affecting the social life of the MOO, but only implement whatever decisions the community as a whole directed them to" (Dibbell 246). The problem with this was, Dibbell laments, "Arguments broke out on **social* [one of the main chat channels] and elsewhere that had only superficially to do with Bungle (since everyone agreed he was a cad) and everything to do with where the participants stood on LambdaMOO's crazy-quilty political map" (246). Like every community, LambdaMOO had its factions.

Parliamentarian legalist types argued that unfortunately Bungle could not legitimately be toaded at all, since there were no explicit MOO rules against rape, or against just about anything else—and the sooner such rules were established, they added, and maybe even a full-blown judiciary system complete with elected officials and prisons to enforce those rules, the better. Others...seem to feel...that it was high time the wizardocracy returned to the position of swift and decisive leadership...

And then there were what I'll call the technolibartarians. For them, MUD rapists were of course assholes, but the presence of assholes on the system was a technical inevitability, like noise on a phone line, and best dealt with not through repressive social disciplinary mechanisms but through timely deployment of defensive software tools. ... Don't whine to the authorities about it—hit the @gag command and the asshole's statements will be blocked from your screen (and only yours). It's simple, it's effective, and it censors no one.

Yet no position was trickier to maintain than that of the MOO's resident anarchists. Like the technolibbers, the anarchists didn't care much for punishments or policies or power elites. ... But their high hopes were complicated, in general, by a somewhat less thoroughgoing faith in technology... And at present they were additionally complicated by the fact that the most vocal anarchists in the discussion were none other than legba, Bakunin [the real-life partner of legba], and SamIAm, who wanted to see Mr. Bungle toaded as badly as anyone did. (Dibbell 247-248)

Irby 6

Note how the issue at hand is not "Did Mr. Bungle commit rape?" but rather "Should we dispense law and order online, and if so, how?" To LambdaMOO, there was no disagreement: Mr. Bungle was a rapist.

If this occurred in more recent years, however (and variations of this event have), there would be no such consensus. Since there is an assumed divide between the Internet and the individual, many (mistakenly) believe that their actions have no real effects on others. Rape, for them, would be explicitly physical and could not occur to a real person through virtual means. Sure, the *avatar* might be raped, but that's not *real*. Mr. Bungle himself had this view, explaining that he was "engaged in a bit of a psychological device that is called thought-polarization... It was purely a sequence of events *with no real consequence* on my RL [Real-Life] existence" (qtd in Dibbell 251, emphasis mine). In other words, LambdaMOO was a game, and all the men, women, and other people there weren't real. They couldn't hurt him, so it stood to reason that he couldn't hurt them—a common defense of online rape culture. And though everyone in LambdaMOO agreed that Mr. Bungle's actions were indeed hurtful, the correct course of action was unclear since the community had never bothered to make any rules post-Curtis's "New Direction"; there were no rules against cyberrape or any other act of violence.

The arguments that were tossed around on LambdaMOO then are identical to the views that many hold on the Internet now. The @gag command resonates with defenders of free speech since there would be no mass censorship of ideas. But this self-policing puts the onus of censoring hate on the victims themselves as they play a never-ending game of whack-a-molester, blocking every commenter that sends a death threat and muting each individual instance of negative, hurtful content directed their way. There's also the statements that unless something is explicitly illegal, it is permitted (the "Parliamentarian legalist types") and that moderators should have permission to rule as they please (the "wizardocracy"). The first is a rather reductive reasoning, as it puts so much faith in the written law that anything that isn't explicitly stated is legal. There's already grey and unclear language in the law that cyber harassers exploit; for example, New York threw out a 2013 case because the harasser didn't send any of the victim's nude photos *to her*, just her employers and family (Citron 143). There's also plenty of problems with words like "extreme" or "clear," which give the investigators a lot of leeway to pursue cases of cybercrime as it suits them: "Oh, this isn't *extreme* enough, and while there's some evidence, it's not a *clear* case of harassment." The same applies to letting moderators do as they please. While they could, in theory, stamp out hate speech and threats quickly, it also depends on the moderator. They could easily state that the behavior doesn't justify any action and do nothing, or they could go the opposite route and ban all instances of certain words regardless of context punishment for all due to the actions of the few.

Also like today, the denizens of LambdaMOO could not agree on what to do with the harasser in their midst. After numerous debates that went nowhere, a rogue wizard toaded Mr. Bungle, putting a definitive stamp of closure on the matter. Of course, this was only a symbolic victory, as the former Mr. Bungle went through "the minor hassle of acquiring a new Internet account, and LambdaMOO's character registration program...simply [treated] the known felon as an entirely new and innocent person" (Dibbell 254-255). Thankfully, "Dr. Jest" never committed any new acts of violence against LambdaMOOers, but his continued presence in the manor only made the facts clear: that player could just keep coming back to the table. This is even truer now, as we don't have to change IP addresses with every ban—just emails and passwords.

This ease with which harassers can generate threats against their targets has only increased with Web 2.0 and 3.0. Most are familiar with the former, as Web 2.0 is the design doctrine that focuses on the creation of platforms where users can create and share content. Social media rocketed to fame as a result. What has turned companies like Facebook and Twitter from being merely hosts of content into the curators of the Internet is Web 3.0—hyperpersonalization, tailoring our experience of the Internet (and the services provided therein) to our individual needs and desires. Depending on one's outlook, this will be a hopeful vision of the future or a corporate-owned dystopia. Siva Vaidhyanathan takes the latter view in The Googlization of Everything, noting that Web 3.0 "entails the harvesting, copying, aggregating, and ranking of information about and contributions made by each of us. This process exploits our profound need to connect and share, and our remarkable ability to create together—each person contributing a little bit to a poem, a song, a quilt, or a conversation" (83). Because we use "free" websites like Google and Facebook in exchange for our data, we become the product that is marketed, sold, and repackaged for us. The more information we give, the better the search results Google can provide. The closer our Facebook profile matches ourselves, the more friends we can find and connect with. And in the meantime, all that data is collected into bundles that can be traded as commodities on the web.

But the most terrifying aspect of Web 3.0 is that all that information can also be given to people who want nothing more than to destroy us. Mr. Bungle may not have known or had the means to know who his victims were, but today's harassers can not only know the faces and names of their targets but also where they live, where they work, what vehicle they drive, and who their friends and family are. The story of Kath Read provides an example of how this wealth of data can be wielded against us. Read, an Australian librarian, has faced harassment for years because of her active support for plus-size people and denigration of Western fat-shaming culture on her personal blog. Then, "one day, Read arrived home and found a note in her mailbox. It read: 'Hi fat bitch, I see this is where you live'" (Jane 54). Another unknown individual signed Read up for "every weight-loss clinic, gym, personal trainer, diabetes clinic ... in Brisbane," which all excitedly called up their new customer for months on end (54). Unfortunately, Read's story is relatively tame compared to others. Kathy Sierra, a once-prominent blogger in Silicon Valley, received numerous emails threatening to kill her. Fearing for her life, she canceled her speaking engagements: "I'm afraid to leave my yard. I will never feel the same. I will never *be* the same" (Citron 36). This show of fear only stoked the ire of more pseudonymous individuals, as the attacks against her amplified to the point that one troll—the infamous "weev"—"posted her social security number and home address all over the web because he didn't like her 'touchy reaction' to the harassment" (37). Many victims have lost their jobs, been run out of their homes, and have vowed to never go online in a world that increasingly demands it.

Worse still, Hate 3.0 (as Citron calls this form of personalized hate) is so widespread and so powerful that many struggle with it years after the events occur. "Google bombing" is a common tactic that harassers utilize to destroy their target's reputation, as they can game Google's search algorithm to promote an "alternative" narrative that paints them in a comically obscene light. One interviewee that Citron talked to noted how her attempts to make a LinkedIn page to promote herself professionally was buried by her abusers: "To this day, a search of her name produces an Autocomplete prompt with her name and the message board's name. If the prompt is selected, the *first* page includes links to the destructive posts with titles suggesting that she is a liar and a racist. Even if users ignore [it], they will see that the fourth entry on the first

Irby 10

page...asks if she is a 'lying bitch'" (69, original emphasis). Not only is this infuriating for the victims to witness, but Google bombing is also why many victims request that employers don't look them up online. Since they have little control over what Google does or doesn't allow in its search results, they have no way of knowing who gets to speak in their stead online.

This is not to say that victims can do nothing to fight for themselves. Those who have many supporters can counter-bomb the Google algorithm, promoting more positive and accurate information about the target to resurface. Even if a victim of harassment starts out with no one on their side, there are many groups dedicated to fighting back against it. Zoe Quinn, one of the most prominent victims of the Gamergate attacks, founded the Crash Override Network, which helps provide employers with more information about online abuse and aids victims in resetting their online reputations and in increasing their security online ("About the Network"). Other groups, such as Anonymous, take even more radical steps to ending online abuse, typically by using the abusers' tactics against them. The online vigilante group used their collective skill to identify a group of rapists that had recorded their attack and shared it across social media. However, such brute tactics also blur the line of legality, as evidenced by how police chose to investigate both the rapists *and* members of Anonymous (Citron 115). The resounding popularity of the #MeToo movement also illustrates how much power those affected by harassment can have when they bind themselves together against sexual and online harassment.

While socially shaming harassers can work to deter them, the proxy war between abusers and supporters of the abused can only go so far before legal action is needed. It is here that I must mention the obvious, that the law has still not caught up with technology. One notable example of this is how the law addresses revenge porn or the uploading of nude photos and videos without the consent of those involved. Often, abusers will upload these with the target's name, address, and phone number. The aim is to bombard the victim with solicitations for sex and, in some of the worst cases, have violent individuals assault them. Victims who want to remove the images/videos will often find that the site administrators will effectively hold them for ransom, demanding large or monthly payments in exchange for their removal. One would imagine that such behavior would amount to libel, extortion, and more, but many have been turned away by law enforcement. Some examples of why the law did not get involved include, "One post amounted to an isolated event, not a pattern of abusive behavior," "The law does not cover nude images that victims take of themselves (self-shots)," and "...revenge porn laws might criminalize speech in which the public has a legitimate interest" (Citron 145, 149-150). And while more states have begun to outlaw revenge porn, the language of the law runs the gamut of being too precise and too broad.

At the moment, three portions of the law that prevent adequate responses to online abuse are the technical knowledge required to persecute these cases, ascertaining the proper punishments and procedures, and free speech. While these are not all the reasons why Hate 3.0 cannot be sufficiently combatted (others include the ideologies that abusers subscribe to and the previously noted ambiguity/strictness of current laws), I focus on these issues as they were the key discussions of LambdaMOO during the "Rape in Cyberspace." By viewing the past and present in parallel, we can see where we have improved and where we still need to grow.

The first to address is that of the legal ramifications of online abuse. The denizens of LambdaMOO did consider getting the law involved. Dibbell writes, "What, some wondered, was the real-life legal status of the offense? Could Bungle's university administrators punish him for sexual harassment? Could he be prosecuted under California state laws against obscene phone calls? Little enthusiasm was shown for pursuing either of these lines of action, which testifies

both to the uniqueness of the crime and to the nimbleness with which the discussants were negotiating its idiosyncrasies" (249). While LambdaMOO residents were more than likely aware

of the legal courses of action they could have taken—the base skewed toward the academic and techno-savvy—it was still very unclear what, if anything, could be done in real space to punish Mr. Bungle for his actions; after all, they didn't even know his real name. If law enforcement were contacted, I doubt that anything would have come of it. As I have alluded to throughout this essay, law enforcement struggles to understand and to coordinate itself against cybercrime. Citron relates how the journalist Amanda Hess had police asking such basic questions as "What's Twitter?" (Citron 144). Here's another example, this time from Jane:

Jessica Valenti dealt with her first wave of rape and death threats by leaving her apartment, changing her bank accounts, and getting a new mobile phone number. When the next wave of hate crashed, she reported the abuse to law enforcement officials. The [FBI's] inspired advice was to suggest she leave home until the threats blew over, to never walk outside her apartment alone, and to be alert about any cars or men who might show up repeatedly outside her door. (Jane 89)

Rather than spending countless resources into uncovering the names and addresses of each individual abuser, the FBI washed their hands of the issue and told Valenti to deal with the issue herself, as if she was the one to blame for inciting the hate! And it certainly doesn't help that male-dominated police forces occasionally dabble in online harassment themselves (Jane 90). Not only do the harassed have to prove to the police that they have a problem that they can't just "unplug" from, but they also have to break through layers of toxic masculine ideals, a culture of rape that prioritizes the "purity" of women and the shaming of those who have had sex, *and* their ignorance of the finer points of technology (such as IP addresses, requesting information from social media sites, and how virtual private networks work) and the law concerning such technologies.

Irby 13

In combination with police inexperience of digital matters, the law lacks a clear understanding of how to handle online abuse. The easy path that has been taken so far is to let the individual platforms take care of themselves. Facebook, Twitter, and Google all have various policies in place to combat harassment, but they are often applied haphazardly (if at all) and typically resort to banning accounts (which didn't work to stop Mr. Bungle and most definitely doesn't stop harassers today). One major point of contention is if punishment should be applied to the person or the online avatar. Brian Simpson, author of "What happens online stays online? Virtual punishment in the real world," argues that cybercrime should be punished via the avatar: "the argument here is that the real person cannot commit the virtual crime without the avatar and the role that it plays in the virtual world. ... In this sense, does it make sense to punish the person in the real world for something they are not in that world? Does it not make more sense to punish the avatar they identify with in the virtual world and so suffer the consequences there?" (12). Simpson does have a point in that people can experience the virtual world differently depending on their avatars, as many have experimented with differing identities, sexualities, and more online. The avatars appear separate from their human controllers.

But I contrast this with the research of Diane Schiano, who found that participants in the ever-changing LambdaMOO "reported...an awareness of social pressures to maintain the authenticity and accountability afforded by a single primary identity. As one person put it, 'pseudonymity is not anonymity'" (Schiano 132). The avatars that people use are often reflections of the person using them, and they can affect their creator in profound ways. Even though Mr. Bungle's assault on Starsinger and legba was contained and constrained by words on a screen, legba wrote her condemnation of Mr. Bungle with "posttraumatic tears...streaming down her face—a real-life fact that should suffice to prove that the words' emotional content was

no mere plaything" (Dibbell 242). And with Web 3.0, the line between avatar and the individual is blurring. Facebook only allows real names (or at least real-sounding names), YouTube viewers reward creators who portray themselves authentically, and LinkedIn is based entirely on the idea that the person's profile is an accurate presentation of their professional progress thus far. To say that punishing the avatar is enough to repay for abuse that is felt physically or emotionally

(which is to say, invisibly physical) is to invite a woefully shallow view of our digital entwinement.

Over the ineptitude of the police and the murkiness of the law, the most difficult and notorious debate concerning online abuse is that of free speech. As I mentioned earlier, many on the Internet vehemently oppose any kind of regulation of speech online for fear of a totalitarian censorship of ideas that "The Man" does not like. To paraphrase Citron, Jane, and just about every survivor of online abuse in the world, nude pictures and social security numbers are not "ideas" to be debated over a cup of tea at dawn. Sending a tweet that threatens to rape and murder are not ideas that need further clarification or can be ignored as harmless "jokes." The marketplace of ideas doesn't need, nor did it ever request, revenge porn and Google bombs. And the First Amendment in the US doesn't protect the following: true threats ("speech intended to convey a serious intent to hurt another person or that a reasonable person would interpret as expressing a serious intent to cause bodily harm"), defamation and libel, revenge porn (in some states, though the number is growing), the intentional infliction of emotional distress, and civil rights violations (Citron 199-225). And even if one could just block what they don't want to hear online, other people often bear witness to it, too. It's the physical equivalent of listening to a man shouting hate at a deaf person looking the other way; while the intended recipient hears nothing,

everyone in the room grows increasingly uncomfortable. The virtual is just as public and open as the real.

Rather than merely summarizing my statements thus far, I would like to conclude this essay with a series of resources for those who have suffered online abuse or would like to protect themselves online in advance. According to the Center for Solutions to Online Violence, enabling two-factor authentication on any account that supports it is an excellent start. Password managers like LastPass and Dashlane also allow users to quickly create strong passwords for each website they visit. CSOV also recommends locking down privacy settings on old Facebook posts, which limits how far harassers can dig for information on your public profile. To see what kinds of information is out on the web already, use an aggregator like Spokeo, which can also issue take-down requests to remove such info. Also remember to delete old accounts if they aren't in use, as they might have information that you still use (like an email address) ("Locking Down Your Digital Identity"). These are just a few steps one can take to defend themselves online until such steps are no longer needed. When that day will be is another question entirely. Like Mr. Bungle, abusers, harassers, and trolls seem to always come back, and they will no doubt continue to do so as long as they have the power to. With stronger laws, greater awareness, and fierce opposition, that power can be taken away.

Works Cited

Citron, Danielle Keats. Hate Crimes in Cyberspace. Harvard University Press, 2014.

- Dibbell, Julian. "A Rape in Cyberspace; or, How an Evil Clown, a Haitian Trickster Spirit, Two Wizards, and a Cast of Dozens Turned a Database into a Society." *Flame Wars: The Discourse of Cyberculture*, edited by Mark Dery, Duke University Press, 1994, pp. 237-262.
- Jane, Emma. *Misogyny Online: A Short (and Brutish) History*. SAGE Publications Ltd, 2017, doi:10.4135/9781473916029.
- Laurel, Brenda. Computers as Theater. Second edition, Pearson, 2014.
- "Locking Down Your Digital Identity." Center for Solutions to Online Violence, http://femtechnet.org/csov/lock-down-your-digital-identity/
- Quinn, Zoe et al. "About the Network." *Crash Override Network*, accessed 24 November 2018, http://www.crashoverridenetwork.com/about.html.
- Schiano, Diane J. "Lessons from LambdaMOO: A Social, Text-Based Virtual Environment." *Presence: Teleoperators & Virtual Environments*, vol. 8, no. 2, MIT Press, 1999, pp. 127–39, doi:10.1162/105474699566125.
- Simpson, Brian. "What Happens Online Stays Online? Virtual Punishment in the Real World." Information & Communications Technology Law, vol. 20, no. 1, Routledge, 2011, pp. 3– 17, doi:10.1080/13600834.2011.557494.

Vaidhyanathan, Siva. The Googlization of Everything: (And Why We Should Worry). 1st ed., University of California Press, Berkeley; Los Angeles, 2012, pp. 82–114. JSTOR, www.jstor.org/stable/10.1525/j.ctt1pn8d3.7.