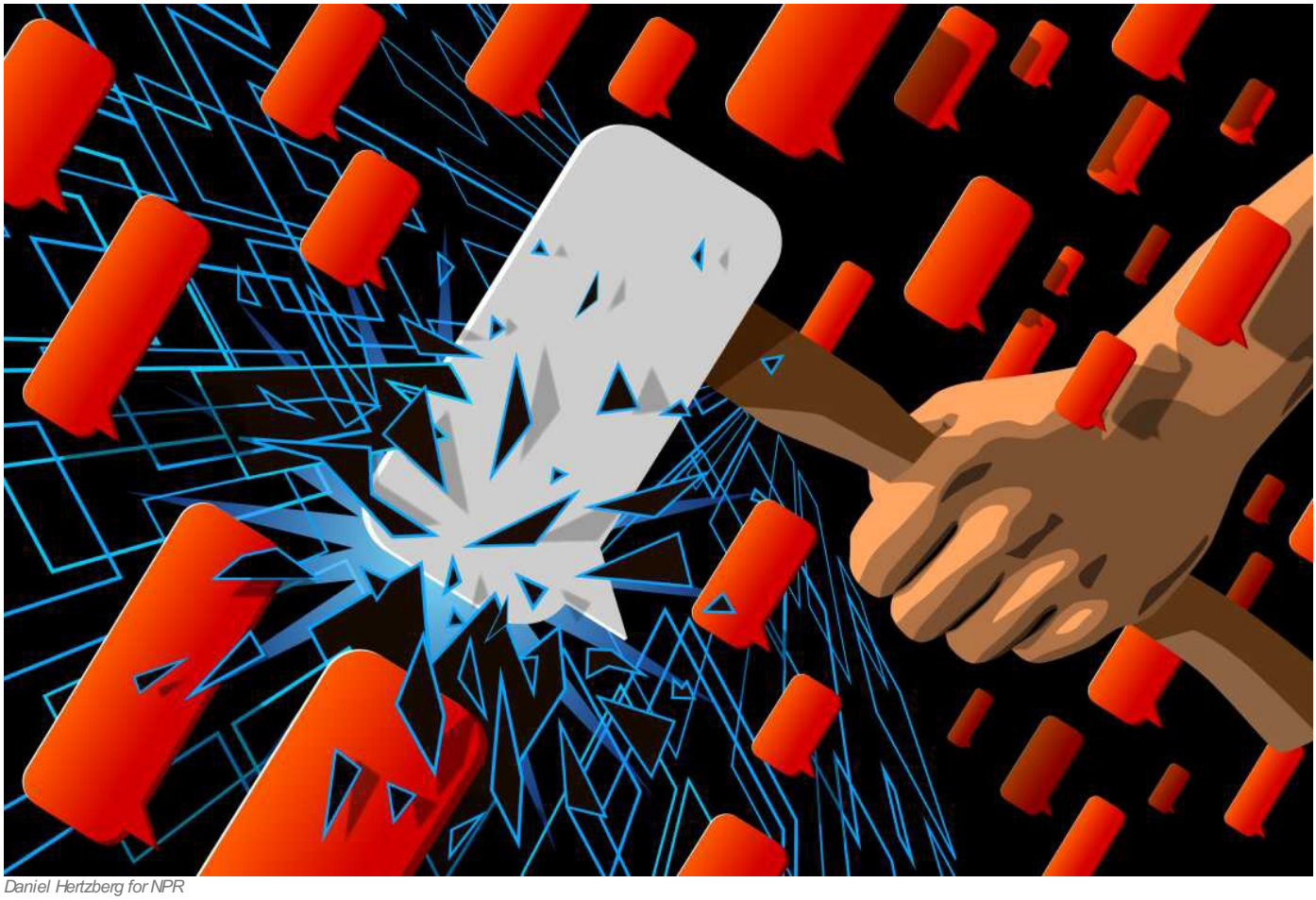
NATIONAL

# How did racist mass texts bypass some anti-spam guardrails after the election?

FEBRUARY 2, 2025 · 5:00 AM ET

Jenna McLaughlin



Daniel Hertzberg for NPR

At the University of North Carolina in Chapel Hill, the mood on campus around the presidential election was "definitely somber," said Samantha Greene, the president of the school's Black Student Movement organization.

But things only got worse once the results were in. Students, including members of the Black Student Movement, started receiving racist text messages in the days after the election from numbers they didn't recognize.

Many of the victims were previously part of pro-Palestinian protests on campus earlier that spring, and were already sensitive about giving out their personal information. They were scared of retribution, violence or being "doxxed" and having their private details leaked across the internet.

Some of their fears were confirmed: The anonymous text messages addressed them by name.

"These text messages sent a shockwave through the community because we were already at a low point," Greene told NPR. "It made those feelings worse, even for those who weren't individually getting those messages. It definitely sent tremors to the rest of us."

They weren't alone.

In the hours after Donald Trump claimed victory in his campaign for a second presidential term in November, Americans across the country started receiving disturbing text messages. Members of Black, Hispanic, and LGBTQ communities were instructed to report to nonexistent nearby plantations to "pick cotton," surrender themselves to fake nearby deportation centers or report to phony reeducation camps.

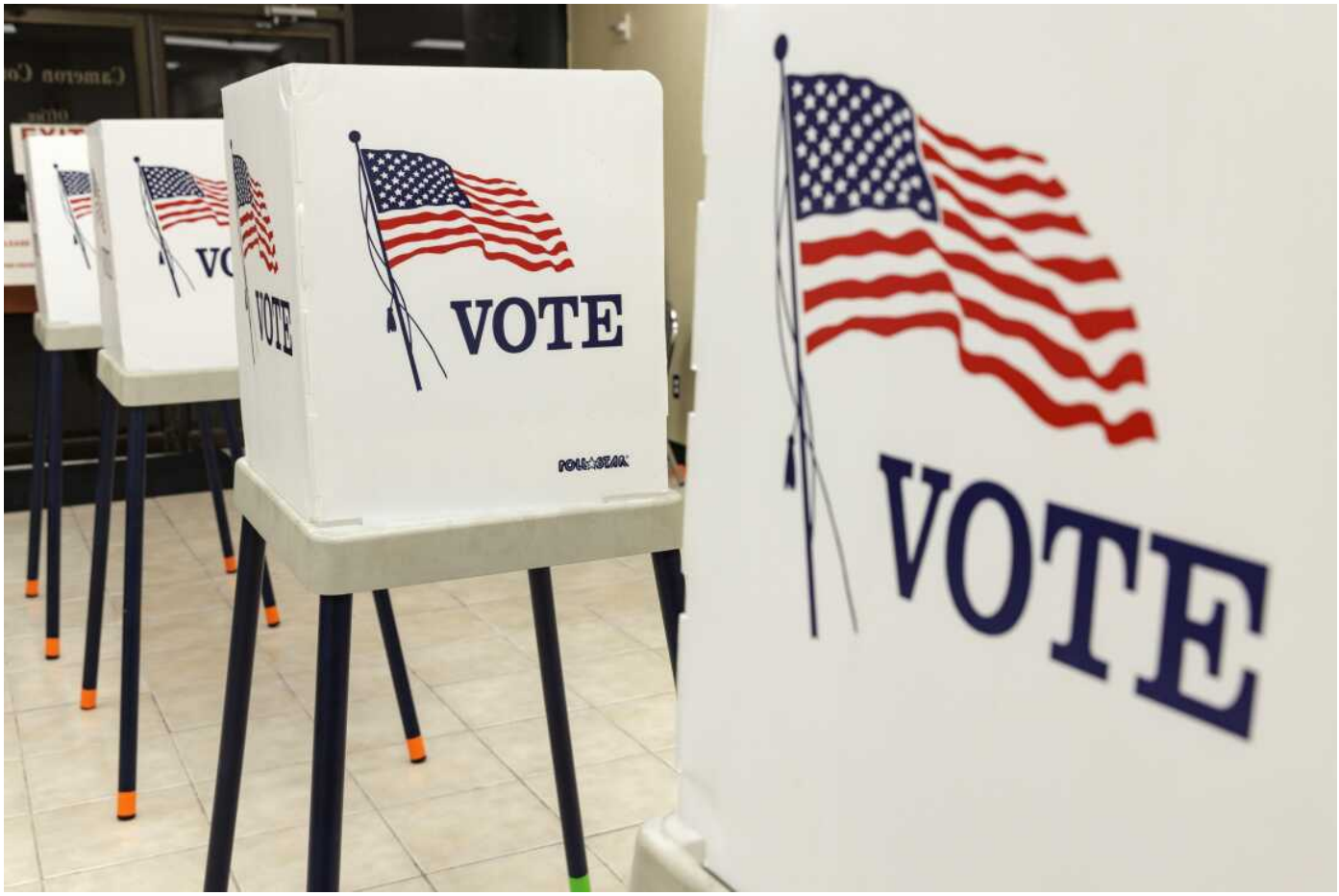
The recipients quickly reported the messages, kicking off a flurry of investigations across the country at the local and federal levels. Those investigations are still ongoing.

In the months since, the victims have largely moved on from the immediate panic caused by the racist texts. But the flood of messages set off alarm bells across the digital communications industry, because they exposed a weakness in the system that could be exploited by bad actors with a range of bad intentions. Three months later, there are still more questions than answers about who was behind the attack and whether the industry is prepared to prevent it from happening again.

### The texts had made it past SMS-messaging guardrails

It took a couple days after the election for the racist texts to become national news, for investigators to understand the true scale.

But in the hours after they were sent, executives in the SMS-messaging industry were already starting to panic.




The Cameron County Courthouse polling place on March 5, 2024, in Brownsville, Texas.
*Michael Gonzalez/Getty Images*

Some of the texts had been detected by spam filters across the messaging ecosystem, setting off alarm bells. But some had made it past those guardrails; they still don't know quite how many. To frustrate investigators further, the messages were mostly coming from anonymous, free, digital number-generating services.

But what they quickly learned was that 15 to 20 different 10-digit phone numbers had flooded the system with vitriolic missives, directly targeting vulnerable young Americans, particularly students in high school and college.

Behind the scenes, the attackers tried and failed to use a number of mass-texting services to deliver their hate before ultimately breaking through the barriers in place.

It quickly became clear to experts in the industry that whoever was behind the texts had made a concerted effort to get their message out, and that it was possible the attack would have serious repercussions for SMS messaging going forward.

That's according to nearly a dozen people across the texting ecosystem who spoke to NPR, some of whom requested anonymity to speak candidly about internal conversations during an ongoing law enforcement investigation.

"What seemed to happen is that there was a determined, thought-out attack on multiple people's systems to see where a chink in the armor was. Then, in a coordinated approach, use all of those to slam out a lot of messages through not just one outlet," said one source familiar with the matter. "This was definitely not a bunch of kids playing."

It wouldn't be the first time.

In the early days of Russia's invasion into Ukraine, Ukrainian Cyber Police investigated a wave of fake SMS messages claiming ATMs were down. Those messages were coordinated with denial of service attacks that took down banks' websites, designed to make Ukrainians afraid they would be unable to access their money. And for a short period of time, it worked.

NATIONAL

**FBI says hateful texts were also sent to Hispanic and LGBTQ community after election**

In the event of a large-scale conflict, having free reign to text Americans directly could cause untold panic.

While sources in the mass-texting industry hadn't previously considered being targets of that kind of attack, they say the example in Ukraine should make investigators take the racist mass-texts very seriously.

"This could be probing activity," the source continued. "It's scary stuff."

## A look at the history that got us here

In the last five years, top U.S. telecoms have joined forces with other companies in the messaging industry to try to eliminate as much spam as possible.

It's a large, complex ecosystem.

First, there's the carriers, like Verizon, AT&T and T-Mobile.

Then, there are companies set up to facilitate messaging, whether that takes place through what industry experts call shortcodes, like the ones used to vote for contests on American Idol, toll-free 800 numbers or 10-digit long codes that look like average American phone numbers.

Companies like Google Voice and Text Now help customers sign up for free or low-cost digital phone numbers, while mass-texting companies, known as campaign service providers, help clients register various kinds of phone numbers to send out informational or marketing text messages through a digital messaging platform.

Finally, there are what's called Direct Connect Aggregators, the trusted middleman that delivers messages directly to the carrier's network.

In the past, it was relatively easy for marketers to sign up for a number and start texting. But over time, carriers were dealing with more and more complaints from users and law enforcement about bad actors that were abusing the system. "Three years ago, [mass-texting] would've been the Wild West," Brad Herrmann, the CEO of Text-Em-All, a mass messaging service, told NPR.

UKRAINE INVASION — EXPLAINED

**Ukrainian hacktivists fight back against Russia as cyber conflict deepens**

The first instinct was to create strict firewalls that blocked any traffic flagged as potentially malicious. But bad actors kept spinning up new numbers and escaping scrutiny anyway. Meanwhile, those restrictions were sometimes overly onerous and ended up blocking legitimate messages.

That's when something called the Campaign Registry was created.

In 2020, the Campaign Registry was founded as a central repository to register, track and coordinate all the different parties in the corporate messaging ecosystem. That way, companies had to register their marketing or informational campaigns in detail, go through vetting processes and receive official authorization to start texting. It's designed to track 10-digit numbers, though there are other, similar bodies that keep track of short codes and toll-free numbers.

The Campaign Registry doesn't monitor or block campaigns itself. Instead, carriers and regulators can go to it for information to help them take action such as blocking bad actors or levying fines.

Slowly, carriers have been shifting towards requiring all corporate messaging to be registered.

"The good news is that all of these systems that have been put in place in the last couple of years are actually pretty good," Herrmann said. "And so, when I heard about [the racist] message getting out, I was like, you know, there's an open door and someone's going to get in big trouble for having that door be open still."

Meanwhile, most companies in the chain have their own spam filters and artificial intelligence systems designed to catch potentially dangerous or offensive messages. It's an extra layer of protection.

Their livelihood is at stake.

The industry came together to fight fraud because text-messaging is a uniquely powerful way to reach people, according to the executives interviewed by NPR.

Marketers can blast out sales to millions, and politicians can recruit voters and volunteers. Public officials can even share or request information en masse, about everything from natural disasters to missing children.

Fraudsters love it too. They keep tabs on people's interests and fears and launch attacks, tricking people into giving up personal information or money through popular scams like fake job postings or impersonating the IRS during tax season.

"The reality is that text messaging works incredibly well," Jon Greenlee, a senior technical product manager at mass-texting company CheapestTexting.com told NPR. "That is extraordinarily attractive to criminals."

Sometimes, it's even more insidious. People use text messaging to directly harass, stalk or issue threats.

Victims of the recent hateful mass-text campaign ranged from descendants of slaves in North Carolina, to middle and high schoolers in more than 10 states and college students at historically black universities, or HBCUs, in the South and Mid-Atlantic.

Students at the historically black Claflin University in Orangeburg, S.C., were shocked and "confused" by the messages they received after Election Day, according to Robert Greene II, an assistant history professor (with no relation to Samantha Greene at UNC.) "Their first thought was, where is this coming from?" he told NPR.

Claflin University was founded in the wake of the Civil War, the oldest institution of its kind in South Carolina; despite the intervening years, racism remains a constant presence in young people's lives in America.

"With our students, they have grown up in an environment where these kinds of messages are pretty commonplace," said Greene. But, he argued, the language of these messages, and the scale at which they were sent, were still shocking. "This idea of rounding up people to be put back in the slavery, things like that. ... It was really jarring, especially with how racially charged this election season was," he said.

The Claflin community quickly realized that they were not alone, widening the mystery.

Students, teachers, and campus law enforcement found social media posts about similar texts being received across the country, Greene recalled. Even the students who "didn't take [the messages] seriously" still wondered how the anonymous user managed to reach so many people at once, he said.

### Some protections did work

Despite the racist messages that were received and seen, many more were stopped. Some of the protections put in place by the messaging industry in recent years did succeed.

For one, the bad actors tried to make use of toll-free numbers but were prevented from ultimately sending out the messages that way, according to one source familiar with ongoing investigations.

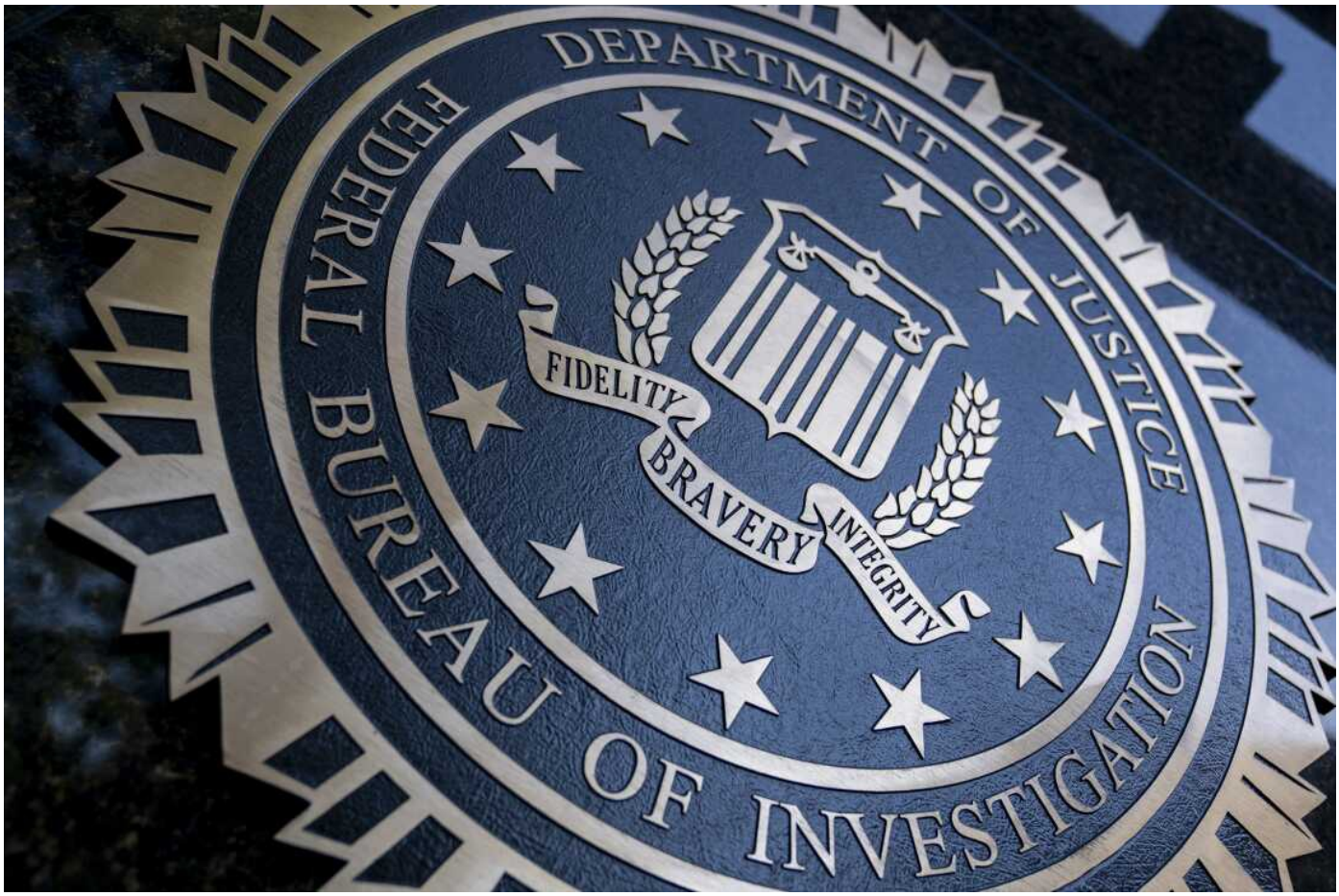
Multiple campaign service providers told NPR that they detected attempts by users to send out messages about plantations and deportations, and those attempts were stopped.

Brad Herrmann of Text-Em-All said bad actors made an attempt to use his company's platform. They managed to create a test account and send the offending message to

themselves. That message set off alarm bells, alerting the carriers who contacted Text-Em-All to get to the bottom of it. Even if it hadn't, the bad actors never officially registered the campaign, so they would never have made it past the trial, Herrmann explained.

Text-Em-All blocked the campaign and quickly changed their policies. Now, users can only send unmodifiable, generic texts during the free trial period.

"This is why we can't have nice things on our free trial anymore," Hermann said.




A seal reading "Department of Justice Federal Bureau of Investigation" is displayed on the J. Edgar Hoover FBI building in Washington, DC, o August 9, 2022..
*Stefani Reynolds/AFP via Getty Images*

NPR also previously reported that a user signed up as "Amy Jones" created a test account through Grand Rapids, Mich., mass-text firm TextSpot. TextSpot CEO Lance Beaudry said its internal AI flagged the language as potentially dangerous or related to human trafficking, blocking the messages from going out. The message was linked to a Philadelphia IP address, but it's unclear whether the attacker was using an anonymizing web-browsing service.

There's some indication the attackers did cloak their location. Louisiana Attorney General Liz Murrill released a statement noting that the state's investigators linked some of the messages received in Louisiana to a VPN beaming the signal out of Poland.

It's difficult to know exactly how many mass-texting services the attackers attempted to use. Of the dozens of companies contacted by NPR, several did not respond to requests for comment about whether there was any indication of misuse during the time period the racist messages were sent out. Meanwhile, some companies might not have insight into every campaign their systems blocked, because some of those

processes are automated.

But based on conversations about the attack, it's clear that the bad actors made several unsuccessful attempts to find flaws in the system before eventually getting their message out.

### The attackers appeared to target loopholes in the system

In addition to hiding their location, messaging executives think the attackers were careful in how they composed the messages themselves.


NATIONAL SECURITY

**Meet the man leading the front-line effort in Ukraine's cyberwar with Russia**


Sources speculate that the messages were artfully crafted to not use specific slurs, possibly sketchy URLs or obviously malicious language that filters would catch.

"This message was kind of unique in that it was able to get past multiple levels of AI and machine learning filters at multiple companies in order to get out," said Herrmann of Text-Em-All.

Attackers might have also been searching for loopholes in the Campaign Registry system – most likely by bypassing it entirely.

The Campaign Registry is focused on monitoring what the industry has called application-to-person messaging, or consumer messaging. Typically, that refers to companies using third-party digital applications to blast text messages to people's phones.

According to the Cellular Telephone Industries Association, or CTIA, communication providers should require companies hoping to send out these kinds of messages to register their campaigns, obtain consent from recipients and provide an option to unsubscribe. The idea is that somewhere along the way, it's likely a malicious campaign would be flagged or stopped.

But there's another kind of messaging that's harder to monitor: personal texts, between friends and family and colleagues.

SMS messaging executives are speculating that it's possible that the bad actors who sent out the racist mass texts either found a way around the registration process, or found a way to blast out messages that looked like personal texts.

"This clearly exposes a weakness in peer-to-peer texting, especially if it can be co-opted by individuals that are looking to send out mass text messages that don't adhere to the regulations that are supposed to be there," said Greenlee.

### For anyone who wants to send a message to a specific demographic, it's not difficult to do

Right now, anyone from a company to an intelligence agency can legally purchase data mined from companies that harvest it, while hackers can sell illegally obtained sensitive personal information for cheap across the globe.

It's an issue that lawmakers like Sen. Ron Wyden of Oregon have personally drawn attention to as a vector for criminals, nation states, activists and companies to abuse. The same way these attackers targeted marginalized communities in the U.S., anti-abortion activists have purchased location data of people seeking reproductive healthcare to target them with abusive messages, according to a 2023 Wall Street Journal investigation.

On Dec. 3, 2024, the Consumer Financial Protection Bureau proposed new rules to prevent data brokers from selling Americans' sensitive personal data like Social Security numbers for illegitimate purposes. The agency cited national security and surveillance risks and potential criminal or violent exploitation as justifications for taking steps to try and rein in the data broker industry.

In the case of these racist mass texts, it's unclear whether investigators will be able to definitively track down the culprits behind these messages, or uncover exactly how they managed to target specific American demographics.

"It would be difficult to prove" data brokers provided the list that the attackers used, wrote Ron Zayas, the CEO of digital privacy firm Ironwall, in an email to NPR. "But what is undeniable is that if you wanted to send out this type of text, or do a lot of nefarious things like phishing emails, disinformation campaigns, or robo-calls and texts, you would most likely start by buying data from data brokers." "Many data brokers will sell just about any data they collect to anyone, without a lot of screening," Zayas concluded.

### Victims of the racist mass text campaign have a lot of questions

Executives in the messaging ecosystem discovered the racist texts after several got flagged by filters. They acted quickly to block the numbers and investigate the culprits. But the campaigns weren't registered, and the trail quickly went cold.

Meanwhile, the damage had been done.

"The atmosphere on campus was incredibly tense," recalled Greene of Claflin University.

Authorities have continued to follow up with him and his students since the messages went out, he said. Samantha Greene at UNC-Chapel Hill said the school administration was less forthcoming with the Black Student Movement. "There's no closure for students," she said.

Regardless, victims of the racist mass text campaign across the country still have a lot of unanswered questions.

The attackers were using free or low-cost digital numbers, disguising their locations and quickly abandoning their accounts.

One of those providers is TextNow, a Canadian company that offers free digital texting and calling. TextNow's openness has many benefits, like allowing low-income users to access communication and government services. But TextNow's platform has been abused in the past for various purposes like fraud, stalking, and fake shooting and bomb threats. TextNow has said it believes the offending accounts were part of a coordinated attack on their system and has since shut them down and is cooperating with law enforcement.

However, sources with knowledge of the investigation tell NPR that the attackers were also using Google Voice, another free or low-cost service that spins up phone numbers. It's difficult to tell if the attackers registered the numbers with Google or other third-party services that sell and manage Google Voice numbers. A Google spokesperson told NPR that "we have clear policies against using our tools to threaten, bully, or harrass, that we apply consistently to keep our users safe." The spokesperson confirmed that in the case of the racist mass-texts, "fewer than 100" accounts violated those policies, and Google "took action."

Now, the messaging industry is scrambling to find out what loopholes the bad actors found, to close them up and prevent something like this from ever happening again.

But it won't be easy.

Even if law enforcement manages to locate the culprits, it's possible they're located overseas. Depending on where they live, it could be much harder to extradite and arrest the perpetrators.

"I see a lot of overseas traffic attempting to gain access to our platform and attempting to send phishing messages primarily," said Greenlee of CheapestTexting.com, the mass-texting company. "What levers do I pull to prevent that access? It's really kind of maddening," he said.

Experts say carriers will lock down any unregistered traffic from businesses, and systems designed to flag malicious activity will only be improved.

But when it comes to texting between individuals, there's a difficult challenge.

"The reality is that text messaging works incredibly well," said Greenlee. "That is extraordinarily attractive to criminals. And the reaction of the industry is, how do we contain this?" he asked. "It's usually problems like this that can trigger change."

Photo of a man holding his cellphone.
*PeopleImages/iStockphoto/Getty Images*

It's unclear what that change might look like, if it comes to pass.

The regulations currently in place for mass-texting are already creating challenges, executives argue.

"What happened was awful, no question," said Ken Rhie, the CEO of Trumpia, another mass text service. "But laws and regulations aren't solutions in many cases." He told NPR he thinks the industry reacted too harshly to the spam problem, and it's blocking a lot of legitimate business. "The measures are often triggering false positives."

It's not just companies using the services.

Herrmann says state and local officials use Text-Em-All to send messages to their constituents about weather emergencies like snow storms or hurricanes. If they don't already have those campaigns registered before storm season hits, they could be waiting to get approved when they can't afford to spare even a few minutes.

More regulation of personal texting could be a tough sell.

Actively monitoring people's personal messages would be very labor intensive for companies, and a potential major privacy violation.

Robots could step in where humans can't. Consumers might be more comfortable with artificial intelligence scanning their messages, especially if it might stop the worst forms of abuse and fraud.

But there will inevitably be questions about how that data is used, how long it's stored, and how vulnerable it might be to hacking and theft.

The U.S. government is currently investigating a Chinese hacking group it calls Salt Typhoon that it says broke into multiple telecommunications companies and stole information about who customers are calling and when, as well as a handful of audio and text records. After months of investigation, the government believes the hackers are either still buried deep in several companies' systems, or could easily break back in.

If more companies were responsible for storing and protecting people's texts and calls, that gives spies and criminals even more opportunities to steal sensitive information.

No matter what, Americans are unlikely to give up their texting.

"SMS is a bit of a precious resource," said Greenlee. "And I think that's why myself and many of my colleagues in the industry are really alarmed and unhappy with the way it's being exploited."

texting | 2024 presidential election | 2024 election | spam

**NPR Network**

**Accessibility**

**Ethics**

**Finances**

GET INVOLVED

**Support Public Radio**

**Sponsor NPR**

**NPR Careers**

**NPR Shop**

**NPR Events**

**NPR Extra**

---