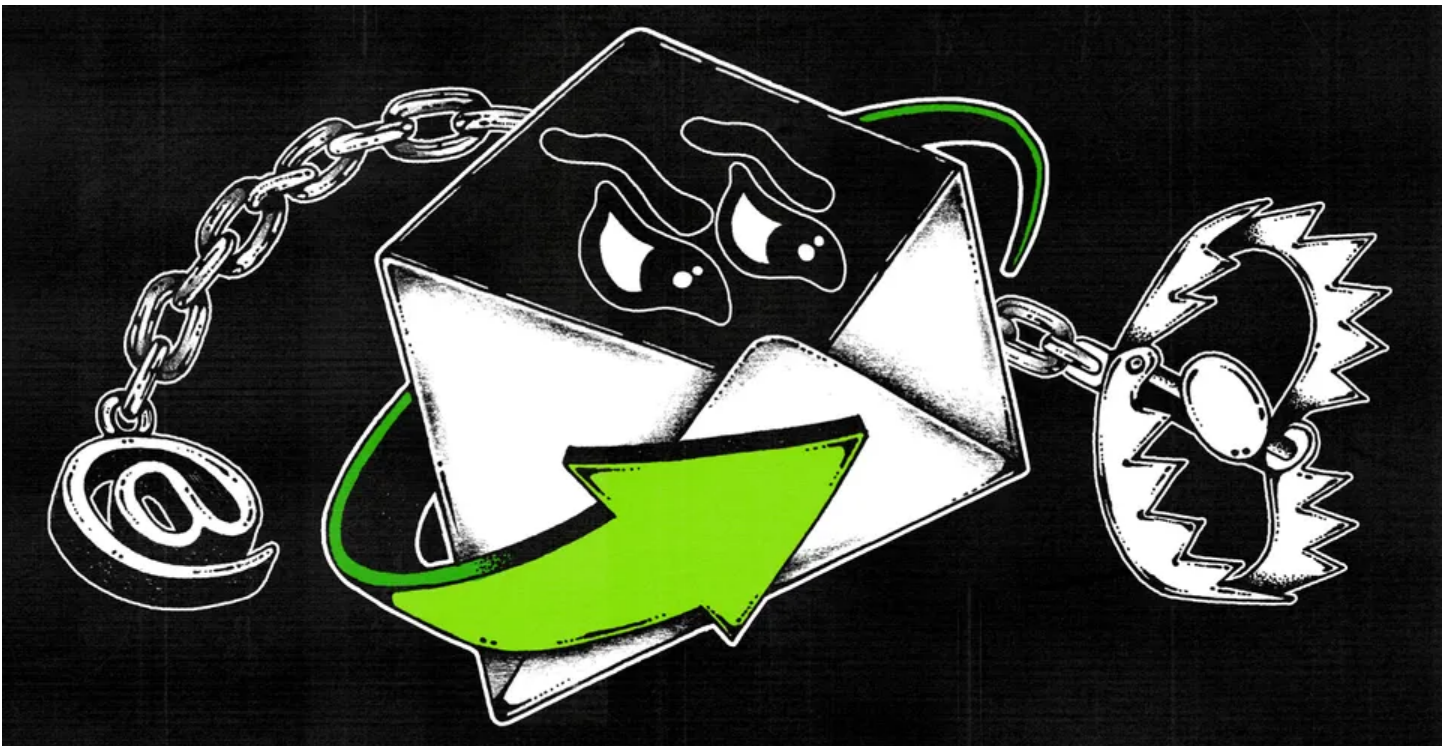# WHAT THE SUPERHUMAN CONTROVERSY REVEALS ABOUT THE SHIFTING ETHICS OF SOFTWARE

The e-mail startup isn't the only company learning that a product can be powerful and elegant without being good.

By Anna Wiener

July 17, 2019

Superhuman, a tech startup, allows users to see when and where e-mails they've sent have been opened. Should individuals have access to that kind of information? Illustration by Kelsey Niziolek

Save this story

In recent months, those attuned to the affinities of Silicon Valley entrepreneurs and venture capitalists have been hearing about a young San Francisco startup called Superhuman. Though its name suggests a <u>nootropics concern</u> or a purveyor of networked exercise equipment, Superhuman's unbodied offering is productivity software for the in-box. Its e-mail client—essentially, it's an interface for Gmail and G Suite—is marketed as a high-powered "email experience"; users speed through their in-boxes via keyboard shortcuts, triaging their messages with assistive algorithms. Superhuman has cultivated the glimmer of exclusivity. To sign up for an account, which costs thirty

dollars a month, individuals who haven't been "referred" must cool their heels on a waiting list. A "pre-boarding" survey asks them to share their employers and job titles. In June, the company's C.E.O., Rahul Vohra, described its user base to the *Times* as "the who's who of Silicon Valley."

On June 30th, someone crashed the party. A Seattle-based designer and tech executive named Mike Davidson published, on his personal Web site, a blog post titled "Superhuman is Spying on You." It focussed on Superhuman's read-receipts feature—a function, at that time enabled by default, that allows Superhuman's users to see when and where e-mails they've sent have been opened by recipients. (It might report, for example, that an e-mail had been read at seven P.M. in Connecticut, then at nine P.M. in New York.) Using vivid examples, Davidson explained why this feature could be dangerous. He proposed a hypothetical scenario in which a woman being stalked and e-mailed by an ex could inadvertently telegraph her location while travelling. A pedophile, he argued, could use Superhuman to track the whereabouts of a child. Recipients of e-mails sent with the feature enabled had no way of knowing that their e-mails were being tracked and couldn't opt out. "Ask yourself if you expect this information to be collected on you and relayed back to your parent, your child, your spouse, your co-worker, a salesperson, an ex, a random stranger, or a stalker every time you read an email," Davidson wrote. "[Superhuman has] identified a feature that provides value to some of their customers . . . and they've trampled the privacy of every single person they send email to in order to achieve that."

Davidson's post immediately went viral, provoking alarm and concern. But it also inspired scorn and derision. On Twitter, industry leaders and entrepreneurs, some of whom were investors in Superhuman, rushed to the company's defense. Many pointed out that the technology that enables read statuses—a technique known as pixel-tracking—is already widely employed by marketers, salespeople, and others who send mass e-mails and want to measure their appeal. (*The New Yorker*, like many media companies, uses pixel-tracking in its newsletters.) Others construed the blog post as a hit piece. "I can understand both sides," Delian Asparouhov, a principal at the venture firm Founders Fund, tweeted. "But there's a strong correlation between the people outraged by privacy and the people that I think are dumbasses in the Valley." (Soon after, Asparouhov released Supertracker, an open-source application that allows anyone to embed tracking pixels in their e-mails or Web sites—an N.R.A. approach to the issue of user privacy.) "This Superhuman 'scandal' is fascinating," Sam Lessin, a venture capitalist, posted. "In 2019 people really don't understand how the internet works and what to be angry about." The theory behind such arguments seemed to be that ignorance of a once obscure but now revealed technology rendered objections to it moot. If users didn't know how a program worked, and later felt deceived, it was their fault for not keeping up.

Pixel-tracking wasn't invented by Superhuman. It has existed for years; the potential for it is built into the way images work online. On the Web, all digital images are stored on servers. When a

Web browser loads an image, it requests it from its original host server. In the process, it reveals information about itself, including its I.P. address. Using that address, it's trivially easy to find information about the computer on which the browser is running—its city, region, and country.

As text-only e-mail gave way to image-rich e-mail, marketers quickly discovered how useful this property of online images could be. The use of image-based "Web beacons" proliferated. Images used for tracking are deliberately hard to detect—often just a single, transparent pixel in size. They are deployed on Web sites and in advertisements and e-mail; Amazon, Facebook, Google, and many other companies use tracking pixels to follow their users from site to site. While some e-mail clients, including Gmail, allow users to disable automatic image-loading, most load them automatically, making it difficult for recipients to opt out.

A few days after Davidson's post, Vohra responded, also on Medium. "When we built Superhuman, we focused only on the needs of our customers. We did not consider potential bad actors," he wrote. (An astonishing admission, in 2019.) He promised that his company would remove location data from read statuses, delete stored historical data, and make the feature an opt-in, rather than a default, for Superhuman users. Davidson, in his blog post, had argued that the inclusion of the read-receipts feature would have knock-on effects. "When products are introduced into the market with behaviors like this, customers are trained to think they are not just legal but also ethical," he wrote. Vohra seemed to concede this point. "All else being equal, the market will generally buy the most powerful tools it can," he went on. "We need to consider not only our customers, but also future users, the people they communicate with, and the Internet at large." All the same, recipients of e-mails sent with the feature enabled still won't be able to opt out, and won't be alerted to the inclusion of a tracking pixel; Vohra suggested that they might protect themselves by exploring the "rich ecosystem of third-party privacy tools."

All of this seems familiar; these days, the ritualized trading of revelation and apology is commonplace in the software industry. And yet the controversy, and Superhuman's limited, imperfect response to it, was a revealing snapshot of this moment in tech. For years, Silicon Valley benefitted from tech reporting that was either breathless and laudatory or simply indifferent. Since the 2016 election, though, tech coverage has grown more skeptical, investigative, and serious—a shift from treating Silicon Valley as a novelty to seeing it as the power center it has become. The industry has been struggling to adjust to being the center of attention on outsiders' terms. Lately, in conversations with entrepreneurs and some tech workers, I've heard complaints about what they perceive as an anti-tech bias in the media. Tech, this thinking goes, is unfairly targeted. (Why pay so much attention to Facebook but not, say, Big Agriculture?) Social media is rife with grumbles of resentment from founders and venture capitalists, who seem to interpret pointed critique or scrutiny as jealousy and hostility. Criticism is seen as punishment for success, rather than attentiveness to

power and influence. Variations on the sentiment that "it's easier to criticize than create" proliferate. Feedback is internalized personally rather than structurally. There is a deepening sense of victimhood.

This defensive response to criticism—even when that criticism comes from someone like Davidson, who is not a member of the media but an industry insider—runs counter to Silicon Valley's much-touted culture of iteration and rapid adaptation. There is a strange fatalism to the argument that pixel-tracking's ubiquity is a testament to its permanence, and to the framing of these technologies, and their misuse, as inevitable. In a professional context, pixel-tracking is a fairly benign tool; it can be used for content marketing, lead generation, or reëngagement. But it takes on a different sheen when it's deployed for personal use. There was nothing inevitable about the extension of this technology into the personal sphere—that was a product decision that Superhuman chose to make. Although there is some evidence that the use of tracking pixels has grown more common in one-to-one correspondence, it is essentially a niche practice; it's still not obvious why productive people should want to track their correspondents the way marketers do.

Superhuman, of course, is not a mass-market consumer product (though Vohra has spoken about "making everybody superhuman" with software that can "democratize productivity"). Like most software products, it is designed to prioritize the specific interests of its own users: in this case, knowledge workers, managers, executives, and entrepreneurs. It's for them that a Superhuman keyboard command called "Instant Intro"—a shortcut that replies-all, moves the original sender to BCC, and drops in a customizable text snippet ("Thanks, Pat! Moving you to BCC")—is an appealing time-saver. E-mail, for this audience, is a chore, or a field of opportunity, at least as much as it's a medium for interpersonal communication. And yet—if you're not a stalker or creep—individual open-rate data is rarely actionable. One might experience anxiety upon seeing that someone has read but not responded to a message; glimpsing a correspondent's e-mail habits, one might enjoy an ambient sense of superiority or leverage. The real value of read statuses may just be a feeling: being privy to other people's data, consensually or otherwise, can create a sense of power or control. There's a certain satisfaction to surveillance. Data isn't necessarily knowledge, but it can feel like it.

At issue, ultimately, is the ethical question of what makes software "good." The qualities of good software include seamlessness, efficiency, speed, simplicity, and straightforward user-experience design. Failing to maximize these values may feel, for a software engineer, like driving a Ferrari below the speed limit—a violation of the spirit of the enterprise. But the seamlessness, efficiency, and power experienced by users don't necessarily translate to positive social experiences; the short-term satisfactions offered by software can upstage its longer-term implications. One of the challenges of ethical software design is that, in some respects, it asks developers and designers to work against themselves and to counteract what makes software so useful in the first place. It's not clear, to

outsiders, how Superhuman decided to build read statuses; the final state of a shipped product is often the aggregation of a series of arbitrary choices made along the way, an accretion of guesswork, experimentation, and technical possibility. No matter how it was made, though, the lack of consensus about whether the decision was banal or egregious reveals a knot in Silicon Valley's internal logic. The defense of technologies like pixel-tracking has long been that they are designed to operate at scale, where they are said to be harmless. But technologies that are useful and morally permissible in that context may be harmful and unethical at the ordinary, human level. The question then is how and when to scale them back.

A previous version of this piece misstated Delian Asparouhov's job title.

[Anna Wiener](#) is a contributing writer to The New Yorker, covering Silicon Valley, startup culture, and technology. She is the author of "[Uncanny Valley](#)."

More: **Email   Silicon Valley   Ethics   Technology**

DAILY

The best of *The New Yorker* today, including essential reads, fiction, humor, and a peek behind the scenes of our biggest stories.

E-mail address

E-mail address

Sign up

By signing up, you agree to our [User Agreement](#) and [Privacy Policy & Cookie Statement](#). This site is protected by reCAPTCHA and the Google [Privacy Policy](#) and [Terms of Service](#) apply.