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.

we focused only on the needs of our customers. We did not consider potential bad actors

had argued that the inclusion of the read-receipts feature would have knock-on effects. 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

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

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.

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.

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. —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.

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.

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.

 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.

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.

Email startup Superhuman [ruffled some feathers](https://gizmodo.com/silicon-valley-s-hottest-email-app-raises-ethical-quest-1836051629) this week thanks to a [viral blog post](https://mikeindustries.com/blog/archive/2019/06/superhuman-is-spying-on-you) by former Twitter vice president of design Mike Davidson detailing how one of the $30 a month service’s core features was actually a run-of-the-mill privacy-violating tracking pixel that transmits information about recipients, including geolocation, back to the sender every time an email containing it was opened.

Now that there’s been a [considerable backlash](https://www.vice.com/en_us/article/a3xpwj/email-tracking-is-creepy-and-invasive-and-no-one-should-do-it) against the firm, Superhuman says it’s canning one of those effective immediately, as well as changing others.

Tracking pixels are often criticized by data protection advocates because they collect comprehensive data about the user, mostly without knowledge of the user. As the tracking pixel cannot be seen with the naked eye, and the common user does not recognize the meaning of the small graphic even when it is visible, the tracking pixel involves a transfer of information without consent.

use of tracking pixels is beneficial for website operators, SEOs and email senders. This is because they can use the information generated to improve their online offers, make them more user-friendly, and adapt the offers to the most commonly used browser types and versions.

Even more advantageous is the fact that tracking pixels are more effective than [cache](https://en.ryte.com/wiki/Cache) in browsers: The access to a page is still counted. If JavaScript is used, more information can be collected. This includes the screen resolution, plugins used, support of certain technologies by the browser, etc. It therefore becomes possible to differentiate between users and bots, as well as create user profiles. The IP address, visits by a certain user, and the properties of this user can be used to create [navigation paths](https://en.ryte.com/wiki/Click_Path). For web analysis, however, the tracking pixel generally just forms the basis. Advanced technologies are required which are only realizable by specialized service providers.

Tracking pixels can also be beneficial in the analysis of sent email newsletters, because they show the opening rates of certain emails or newsletters through the user statistics data. Together with [A/B tests](https://en.ryte.com/wiki/AB-Testing), successful campaigns can thus be determined. From the recipient’s point of view, this has the advantage that newsletters in the future can be designed to be more relevant and interesting.

The mainstreaming of digital vaccine passes could lead to more surveillance, privacy researchers cautioned.

Many developers said they had taken pains to make sure the passports do not cross privacy boundaries.

officials said in January that data from the country’s coronavirus contact-tracing system had been used in a criminal investigation, even though leaders had initially said it would be used only for contact tracing.

Some business groups and companies that have adopted vaccine passes said the privacy concerns were valid but addressable.

The measures faced strong resistance from computer scientists, privacy groups and civil-liberty lawyers because the features represented the first technology that would allow a company to look at a person’s private data and report it to law enforcement authorities.

once the ability to sift through users’ private photos was out there, it would have been ripe for misuse. Governments, for example, could potentially lean on Apple’s technology to help track down dissidents.

great that they’re taking a moment to think things over,” but that he and other privacy coalitions would continue to plead with Apple to abandon its plan altogether.

Market researchers are willing to pay brokers for a huge array of data, from dating preferences to political leanings, household purchases to streaming favourites

So the choice was whether to keep mum, he said, or to publish the method so that data vendors can secure future data sets and prevent individuals from being re-identified. It’s always a dilemma

The consensus so far is to disclose. That is how you advance the field: Publish the code, publish the finding

The balance is tricky: Information that becomes completely anonymous also becomes less useful, particularly to scientists trying to reproduce the results of other studies. But every small bit that is retained in a database makes identification of individuals more possible.

The implications of this fundamental shift in the underlying philosophical framework regarding data privacy protection will be profound in the years and decades to come.

the European Union (EU) have long pursued a rights-based regime for protecting personal information. Historically this philosophy holds that data privacy is a fundamental human right. Individuals effectively own their personal information, and who can use it is a matter for them to decide.

Europeans had a “right to delist,” meaning that individuals, corporations and even government officials could request that material be removed from Google’s search results, if deemed “inaccurate, inadequate, irrelevant or excessive,” and not related to discourse regarding the public interest.

There is no “right to be forgotten” in the abstract; no law can ensure that, and no law can be limited to that. Instead, the “right” this aims to protect is the power to suppress speech — the power to force people (on pain of financial ruin) to stop talking about other people, when some government body decides that they should stop.”

The Texas attorney general filed a privacy lawsuit against Google on Thursday, accusing the internet company of collecting Texans’ facial and voice recognition information without their explicit consent.

Google’s indiscriminate collection of the personal information of Texans, including very sensitive information like biometric identifiers, will not be tolerated,

the products violated the rights of both users and nonusers, whose faces and voices were scanned or processed without their understanding or consent

But for the Court to outsource to Google complicated case-specific decisions about whether to publish or suppress something is wrong. Requiring Google to be a court of philosopher kings shows a real lack of understanding about how this will play out in reality.

It’s a pragmatic solution. This speed-bump approach gives people a chance to grow and get beyond these incidents in their pasts.

The Internet’s unregulated idyll seems to be coming to an end, at least in Europe. family brought suit against it and the two employees who leaked the photographs, on a variety of grounds, including negligence, infliction of emotional distress, and invasion of privacy.

The breach, privacy experts say, underscores the delicate balance the cloud computing platforms have struck between security and efficiency.

The largest “clouds” are run by the likes of Amazon, Microsoft and Google, and store data on hard drives. While this increases the free flow of data, it also expands the potential of hackers to loot data.

The evolution of cloud security and data encryption is being driven by some of the industry’s top computer scientists, hired out of the world’s best scientific universities and the National Security Agency.

That new wrinkle — insider information — is a formidable challenge across the industry.

“Financial Institutions need to take all the normal precautions and now a new one, where an ex-employee of their cloud hosting provider could prove to be a threat,” Atlantic.net’s Mr. Puranik said. “They know the intricate details of the architecture and how to exploit the small nooks and crannies for any weaknesses.”

FBI took [disruptive action](https://www.justice.gov/opa/pr/justice-department-announces-actions-disrupt-advanced-persistent-threat-28-botnet-infected) against a Fancy Bear campaign known as “VPNFilter” which targeted routers and network storage devices with malware with destructive capabilities of “bricking” a device by deleting firmware and rendering the device unusable. That campaign especially targeted Ukraine, a favorite target of Fancy Bear.

Many companies now want to cohabit again with their remote employees.

Many remote employees have discovered they're quite happy working remotely and eschewing the commute. And, well, the need to dress up and act as if they actually like their coworkers.

The goal of hacking is to manipulate digital devices in order to cause damage or corrupt operating systems. It also allows hackers to collect user information, steal sensitive information and documents or perform other disruptive data related activities.

While hackers can be both ethical and malicious, most fall within three main types of hacking. These three main varieties of hackers are authorized, unauthorized and grey-hat hackers. Each type has different intents and purposes for their exploits. Let's explore each of these types of hackers and how they operate.

Grey-hat hackers are individuals who exploit security vulnerabilities to spread public awareness that the vulnerability exists. While these hackers do not share the malicious intent commonly attributed to unauthorized hackers, they also don’t necessarily adhere to a code of ethics like authorized hackers.

Ethical hacking often involves many different facets of the information security field. This role requires a lot of knowledge and expertise, from coding and programming to penetration testing and risk assessment. There is a lot to learn within the ethical hacking career, but it’s a high-demand field that will only continue to grow the more technology is used in our world.