Subscribe





Weekend Interview

Signal's Meredith Whittaker: The Push for Online Safety Risks Mass Surveillance

The president of the encrypted messaging app says autonomous AI agents, device scanning and digital advertising are converging into a new architecture of surveillance.

By Mishal Husain

Illustration: Uli Knörzer for Bloomberg; Source Photo: José Sarmento Matos/Bloomberg

June 19, 2026 at 1:00 PM GMT+8

Gift this article

Meredith Whittaker has spent years arguing that privacy is a prerequisite for a free society. As president of the nonprofit foundation behind the encrypted messaging app Signal, she now finds herself defending that principle against mounting pressure from governments and tech companies alike. Whittaker says business models that rely on data collection, the rise of AI assistants and even well-meaning efforts to protect children online risk undermining private communication – and explains why Signal would rather leave a market than weaken encryption.

This conversation has been edited for length and clarity. You can listen to an extended version on The Mishal Husain Show podcast.

You worked at Google for more than a decade. I get the impression that by the end of your time there, you were a thorn in management's side — organizing walkouts on ethics issues.

People who would like to put the goals of infinite profit above the reality of the harms on the road ahead don't like people who point that out.

It wasn't Meredith v. Google. This was a groundswell from thousands of people within the company, echoed today: DeepMind's employees just [moved to] unionize, OpenAI employees [are] beginning to organize in preparation for the IPO.

There is sentiment within and outside tech that is concerned with the fundamental question that [cannot] be avoided: *How do we make sure that we are collectively governing this powerful technology so those who would do harm aren't those in control? How do we scrutinize it? How do we put guardrails on it? How do we determine where it's used, where it's not used, how it's developed and what the goals of that development are?*

Those are questions that every world leader, government [or] community considering a data center needs to be looking at. [1]

[1] The extent of Whittaker's activism within Google intrigued me as I prepared for this conversation. Bloomberg described her as a "Google protest leader" when she departed the company in 2019, citing her role in organizing walkouts involving thousands of staff and contractors. The movement began

in 2018, when Whittaker spearheaded an open letter to CEO Sundar Pichai over Google's involvement in a Pentagon initiative known as "Project Maven." The AI-assisted "Maven Smart System" has most recently been used by the US in Iran, where one of the early strikes reportedly killed more than 100 school children.



The Mishal Husain Show
Meredith Whittaker

0:00/0:00

The core promise of Signal is end-to-end encryption, which means only the sender or receiver can see the actual content of messages. How is that different from WhatsApp, which also has the same promise?

The core promise of Signal is that in the digital world – where almost every micro-action is surveilled, turned into data, processed, modeled [and] sold – we preserve the fundamental human right to private communication, which has existed for hundreds of thousands of years. If you and I are talking, that conversation is gone once we part ways. We have moved into a world where that is no longer true.

We can't live a full dignified life – with the ability to question authority, have different relationships with people, test ideas [and] blow off steam – if we don't have private communication. You can't do military strategy, human rights work [or] journalism. Signal provides that in as robust a way as we can.

We developed the Signal Protocol that moved the field forward in 2013 [and] protects message content. Signal [also] applies encryption to protect *metadata* – your profile photo, name, who you talk to, when you talk to them, who's in your groups [and] how often you chat. WhatsApp *does* collect that; we don't. We go out of our way to collect as close to no data as possible.

We have to expand beyond the application and look at WhatsApp being owned by Meta. Meta is a massive data-collecting entity. Surveillance advertising is the heart of their business model. You message your oncologist: *Let's join that data with all of the other data we have in hand. We*

have Facebook data. We have Instagram data. We have powerful AI models that can find patterns. [2]

[2] We asked Meta to comment on Whittaker's characterization of its business model and approach to privacy. A spokesperson for WhatsApp responded: "We also look at privacy beyond encrypting messages. We don't keep logs of who everyone is messaging or calling. We do not track the messages people are sending one another for ads. We do not sell user data."



Meredith Whittaker addresses Google colleagues at a 2018 rally in New York *Photographer: Bebeto Matthews/AP*

Surveillance advertising is a very inflammatory way to put it.

It's a technical descriptor. Targeted advertising based on the collection of data that purportedly reveals certain qualities of you, and what you might like.

This data is extremely revealing. There's a woman who went to jail in the US because Meta turned over DMs on Facebook Messenger that showed her helping her daughter access reproductive care in the state of Nebraska. [3]

[3] The full story in this harrowing case is that a mother and her daughter were both sentenced to jail after the daughter, then 17, used abortion pills to end a pregnancy at 28 weeks – eight weeks beyond Nebraska's legal limit at the time. The mother was convicted of providing an illegal abortion, while both were convicted on charges related to concealing or tampering with human

remains. A Meta spokesperson later said there was no mention of abortion in the "valid warrants" it received from law enforcement.

I don't know if you saw Bloomberg's recent reporting that a US government investigation into allegations that WhatsApp *could* access encrypted messages was abruptly closed down. An investigator at the Commerce Department reportedly concluded that Meta stores and can view WhatsApp messages.

I saw that news cycle, but I have no inside information to share. I didn't see any evidence that would lead me to believe [that] on a technical level.

Meta always denies that such a power is possible within WhatsApp, but given it's built on your code, I wonder if it makes you curious about how the code is used? Your code is open source. Their version of what they do with it is not.

I think open source should be the floor for the infrastructures that we are trusting with so much in our lives. [4]

[4] Signal was founded in 2014 by Moxie Marlinspike and became a nonprofit foundation in 2018 with the arrival of Brian Acton, a co-founder of WhatsApp who left after its sale to Facebook. Signal's encrypted messaging protocol remains open source.

Do you find it frustrating when you see people *not* care about their privacy?

I find it frustrating when the argument that *No one cares about privacy* is leveraged by these firms to justify what they're doing.

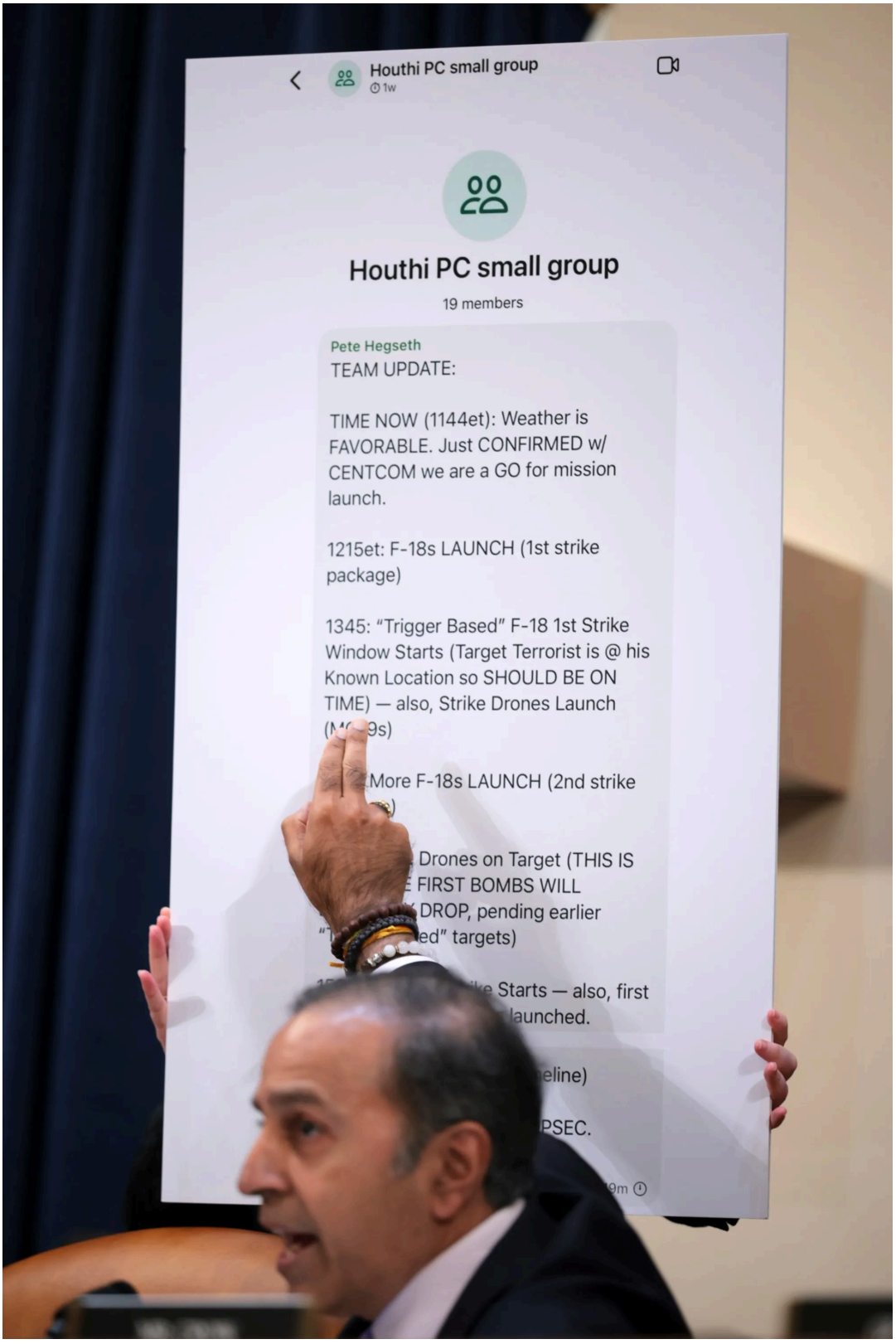
I don't believe that people don't care about privacy. I believe the stakes are very obscure, and we're living in a world where thinking about data flows and privacy legislation is probably pretty far down our list of concerns.

You had two big moments in the growth of Signal: when Edward Snowden trusted it to talk to journalists about government surveillance, and Signalgate, when a journalist was added to a supposedly highly classified Trump administration discussion on military action. When the second happened, what did you think?

I thought, *Whoa, what's going on this morning*? The article hit my feed. I had to read it twice to really let it sink in, because it read almost like a telenovela.

What I didn’t anticipate was that Signal would become a main character. I was concerned that Signal was being spoken about by millions of people who weren’t familiar with the intricacies of encrypted messaging. I wanted to prevent misinformation that could hinder Signal.

This was ultimately men’s thumbs doing things. That is not something an application developer can take responsibility [for].



Leaked Signal messages between members of the Trump administration are displayed during a House intelligence hearing on March 26, 2025. *Photographer: Kayla Bartkowski/Getty Images*

Was it good for numbers?

Yeah, it turned out well for us. We saw growth across the world, and we've seen pretty steady growth since then. [5]

[5] Signal told us it employs about 50 full-time staff, all working remotely, and that its app has been downloaded or installed hundreds of millions of times.

Can I ask how you reconcile yourself with your product being used by people to do harm to others — particularly child sexual abuse? If abusers are using Signal to circulate images of children, that can happen without fear you will hand over data to law enforcement.

We go out of our way to *not* be a social media company. We could pump our numbers fairly easily if we added things like broadcast channels or features that allowed you to find people with similar interests and meet strangers on Signal.

Signal has made a very conscientious choice to stay in our narrow lane as an interpersonal communications app. You have to *encounter* the person you're talking to in some capacity.

But once you do find that person, you can be sure that anything you share with them is free from outside surveillance.

That is Signal's promise. We cannot collect that data [or] turn [it] over, but we limit features that allow mass distribution.

I also need to make a fundamental point: Encryption either works for everyone or it works for no one. There is no way to have a golden key or a special backdoor or access just for the good guys.

Do you struggle with that — knowing that there will be people who are using it for the most abusive possible images of children?

The fact of child sexual abuse is horrifying to me, absolutely. We need to take that so seriously. As a society, [we] need to get much better with looking gnarly problems in the face and actually tackling them.

I also struggle with the persistent focus on privacy as the purported barrier to solving these issues, when we have most of the Epstein list walking around without consequences. We have so few mechanisms to actually help children when they report a powerful figure in their community.



Get the Bloomberg Weekend newsletter.
Big ideas and open questions in the fascinating places where finance, life and culture meet.

Sign Up

By continuing, I agree to the Privacy Policy and Terms of Service.

The UK government is moving towards making it compulsory for tech companies to ensure children can't take or share nude images through their platforms. Is that workable? [6]

[6] Since Whittaker and I spoke, Keir Starmer has focused on another aspect of his tech agenda: banning social media for under-16s. But with his authority weakened by a series of resignations, the prime minister may not be in a position to see those plans through, and has faced questions on whether he is rushing to advance the policy in the face of a possible leadership challenge.

There's never been more data accessible to law enforcement than there is now. Were law enforcement well-funded, were social services well-funded, they could act.

We need to recognize that there are some tools that are not being picked up, and there are some tools that seem an obsessive focus of politicians who like to abstract these very difficult problems into the technical domain and pretend there is one technical fix to solve a problem that needs a social solution.

Let's imagine this tool is one of many. What do you think of it?

Keir Starmer announced what seems to be a fairly hasty proposal.

Our position on client-side scanning is that this constitutes very dangerous mass surveillance. Having a scanning system on your device that is going to purportedly detect nudity can easily be weaponized by governments.

We don't understand the technical mechanism by which this would be implemented. My assumption is we would be looking at a system that would likely "phone home" – send data to governments [and] tech companies – and ultimately comprise a mass-surveillance system of permitted speech that would be implemented across everyone's device, and pose real threats to Signal's ability to provide the robust privacy guarantees that people around the world rely on.



Keir Starmer gives tech firms an ultimatum over explicit images during a speech on June 8, 2026. *Photographer: Carlos Jasso/Bloomberg*



Meredith Whittaker visits No. 10 Downing Street to discuss Signal's concerns with Keir Starmer's team on June 9, 2026. *Photograph: Courtesy Meredith Whittaker*

With all of the big brains in tech, you really don't think it's possible to refine the product in a way that protects children without these massive repercussions?

Part of being a big brain in tech is really understanding the nature and limits of what technology can do. This isn't a question of *Go think harder, nerds*. There is no technology that has been shown to do this in a way that is robust and safe.

I wonder how sustainable your position is. It's not only the UK government that's really concerned on this front — the European Union also had temporary legislation, which just ran out, essentially asking tech companies to voluntarily scan their platforms.

We've taken the same position on that.

If this is the way governments are going, can you imagine Signal not being available in the UK or the EU?

Our position is we would rather exit a market than undermine the technical guarantees that people trust for their privacy. That doesn't change based on jurisdiction; it doesn't change based on year.

That's not something we take lightly – we're not just flexing or being recalcitrant. A backdoor in any market compromises a door into Signal that would be weaponized by nation-state adversaries that are consistently searching for vulnerabilities in our code.

Who do you mean?

Any government with a capable intelligence agency is spending some effort looking at Signal.

Including your own government?

I don't have clearance to know that for sure.

I'm just wondering if you mean Russia? China? Or governments in the West?

It has been represented to us that Russia will pay you if you can find a vulnerability they could exploit.

If you look at the people who rely on [Signal] – heads of state, government officials, military strategists, investigative journalists, people reporting corruption – we need to recognize people have vested interest[s] in infiltrating those networks.

It would be an absolute breach of duty of care were we to implement a backdoor in Signal. We're a nonprofit. We are not a tech company juicing numbers to IPO and exit.

That's one of the intriguing things about Signal. You have some big donors and users who donate to you. What are your annual running costs?

It's about $50 million a year. [7]

[7] Signal has been open about this breakdown, explaining that its costs include labor, renting server infrastructure (it says only a few companies can afford to purchase all the computing power they require), and fees charged by mobile phone companies for SMS verifications. As it does not sell data, Signal says it cannot recoup those costs.

Do you fall short in donations?

We're sustaining. It's about 70% large donors, 30% people who use the app and donate $5 a month, $20 a month. We love them.

Does it feel like a struggle?

It's something I think about a lot. The economic engine of the tech industry is the collection and monetization of data. Signal exists to do exactly the opposite. [That] means we have to choose a different model – one where we don't have a VC saying, *You're not going to get your Series B if you don't figure out how to monetize* [or] shareholders saying, *Figure out how to carve out some data collection so you can build an AI model [and] continue to meet and exceed market consensus.*

What would you like us to be aware of in privacy terms when we use large language models like ChatGPT and Claude?

These are not your friends. These are not conscious beings. These are not sentient interlocutors.

They're very useful.

Sure. Many things are very useful.

You can delete chats and say you don't want your chats to be shared.

You can say all sorts of things, but ultimately, the power to determine whether that happens or not is in the hands of the entity that is running that service.

[Chats] can be stored, logged, mined for more data [and] tweaked slightly to calibrate the responses to your purported preference on behalf of, say, advertisers. Instead of showing ads, perhaps you say, *Find me a very cheap flight*, and it finds you one with their preferred advertising partner that is not cheaper. [8]

[8] Open AI has been introducing ads within ChatGPT for some users, but says they do not influence responses and that the company does not share conversation data with advertisers.

Do you use them?

I ask them to format a document here and there, but I have no relationship with them. I don't ask them questions. I'm very serious about my thinking and writing, and I don't want the process of working through an idea – the struggle of not knowing and then figuring it out – to be foreclosed or eclipsed by the response of a system that's averaging what's already out there.

The next generation of these models is the autonomous personal assistant. [Microsoft AI CEO] Mustafa Suleyman said to me, *You could be buying your Christmas presents in 2026 through Microsoft Copilot*. What do you think of autonomous agents being in people's lives? What would it mean in privacy terms?

Let's take Mustafa's little vision of AI Christmas – I can't wait. *Everyone's getting a gift certificate to Microsoft Copilot*.

What would that mean? I say, *Hey, Copilot, I don't want to live my life. I would like you to live it for me. I don't want to think about the warm feelings I have for those I'm buying gifts for. I would like you to consult with my siblings' group chat and see what our family might like. I would like you to buy those gifts. I would like you to figure out how to get them to the right place.*

That would need access to my credit card, my browser, my Signal, the ability to message my siblings on my behalf, my home address [and] my calendar. What you've just described is a system with very pervasive access across multiple applications and services.

In the context of Signal, it would constitute a kind of a backdoor.

Is this an existential threat to Signal?

I do worry. Any one of the operating system vendors that decides to implement an agent with these capacities is ultimately hollowing out the ability for Signal and others to guarantee privacy or data protection. This is a quiet but profound shift that we are witnessing.

We have three companies in the world with control over our core operating systems – Google with Android, Microsoft with Windows and Apple with iOS. They can make decisions by fiat that fundamentally harm our collective cybersecurity, take away any choice we might have for privacy, and completely hamstring developers building different services.

We are seeing a move of agency away from the application layer – the consumer, who uses these devices – back into these centralized companies.



Whittaker spoke to Mishal Husain in London on June 9, 2026. *Photographer: Jose Sarmento Matos/Bloomberg*

What do you do in your own life? Signal for messaging, what else? When you go for a run, do you put it on Strava?

No, [but] the fulcrum of leverage for me is not individual consumer choice. I am not trying to be a holier-than-thou purist. I have a tracking app I use for health metrics – it's been helpful for me.

That's health data that will be used.

Yeah, and I benefit from that.

I think the lever we need to be pushing on is *systemic* change. I am not going to opt out of life. I am not going to go live in a cabin in the woods and pay someone to print out my emails at the post office so I can feel private.

If we look at Signal's privacy promises, we're not talking isolation from our social, economic [and] political lives – living in a vacuum. We're talking about the ability to *talk* to other people. I have Instagram. I have the NTS

app – it's a really good web radio. Maybe they collect data. I am a person living in 2026 and I want to participate in the world.

What I don't believe is that participation should be on the terms of a handful of tech companies located in the US whose choices are made based on a desire to maximize revenue

Yet, you too are American tech.

[*Laughs*] The irony abounds. [I'm] a complex individual. [9]

[9] Calls to "unplug" from US tech companies have been growing in Europe this year, amid fears that President Donald Trump will use those companies as a source of leverage. European governments are reportedly moving officials off Signal and WhatsApp onto in-house messaging services, Finland has scrapped plans to move election data onto Amazon servers, and European companies such as SAP and ASML have been pouring billions into home-grown AI startups and services.

But I think you're saying to us, *make better choices*, or just *think more carefully about your choices*?

You're not stupid. The choices offered maybe aren't the choices you want. Dream a little bigger. What do you want from these companies? What world do you want to live in?

Do we want tech in our education system? How do we work to guarantee that we're actually using it to shape that better world and not simply *being* shaped by decisions made on a whiteboard in Mountain View by a handful of product managers who really have to ship AI this quarter or they're not going to get promoted?

Who you probably know because you once used to work with them.

Yeah, and they're all named Mike. [*Laughs*]

You never miss that world? It's big bucks, apart from other things.

You mean, *Am I sad I'm not "rich-rich"*? No, I'm "hood-rich." I'm happy being "hood-rich." I don't need to be "rich-rich."

What does "hood-rich" mean?

Rich in the context of the neighborhood you've come from; not rich in the context of complaining about the champagne on your private flight. Don't

cry for me. [*Laughs*]



Mishal Husain is Editor at Large for Bloomberg Weekend

With assistance from
Jessica Beck and Louisa Lewis

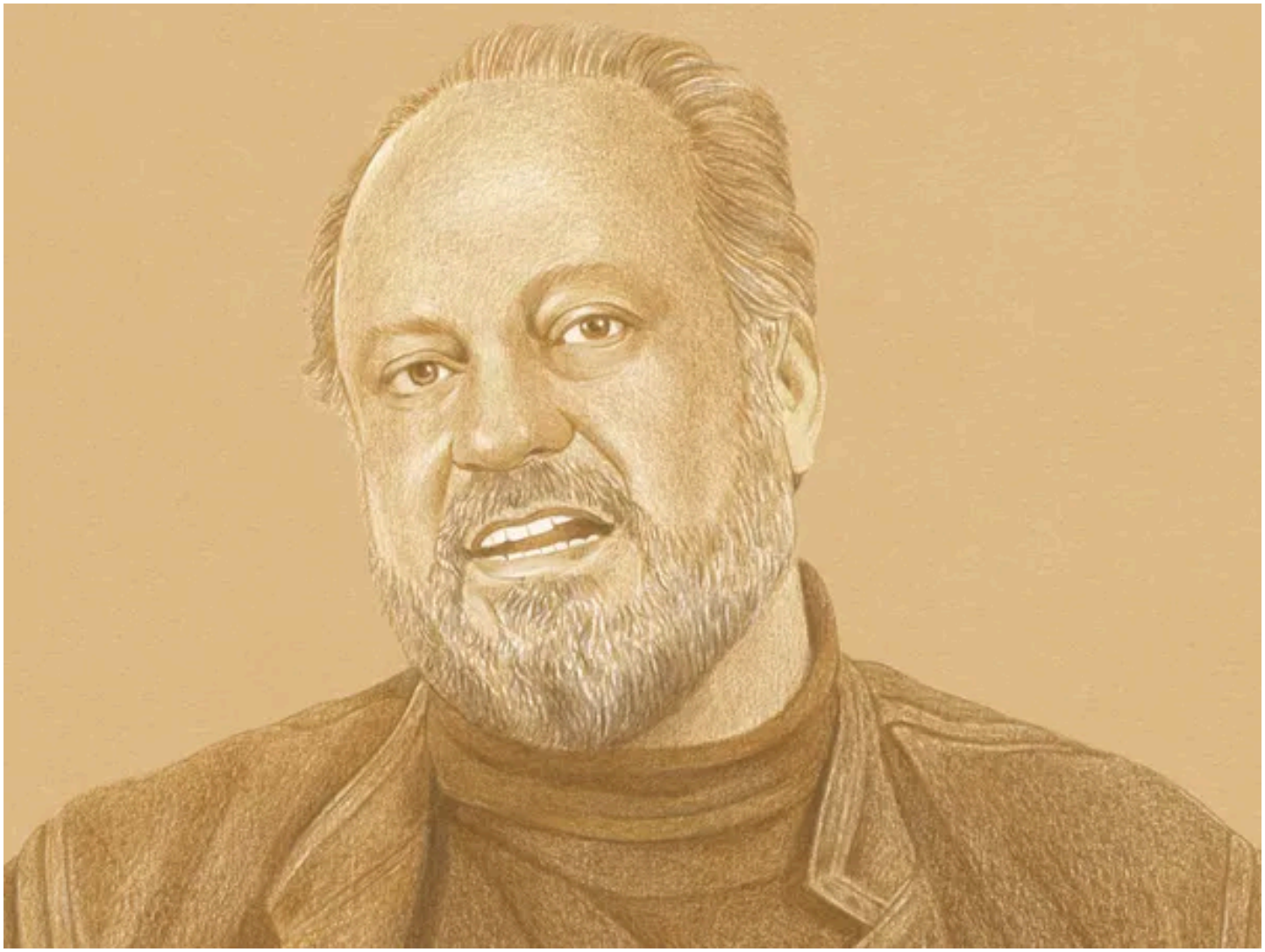
Editors
Kira Bindrim and Chris Martlew

Gift this article



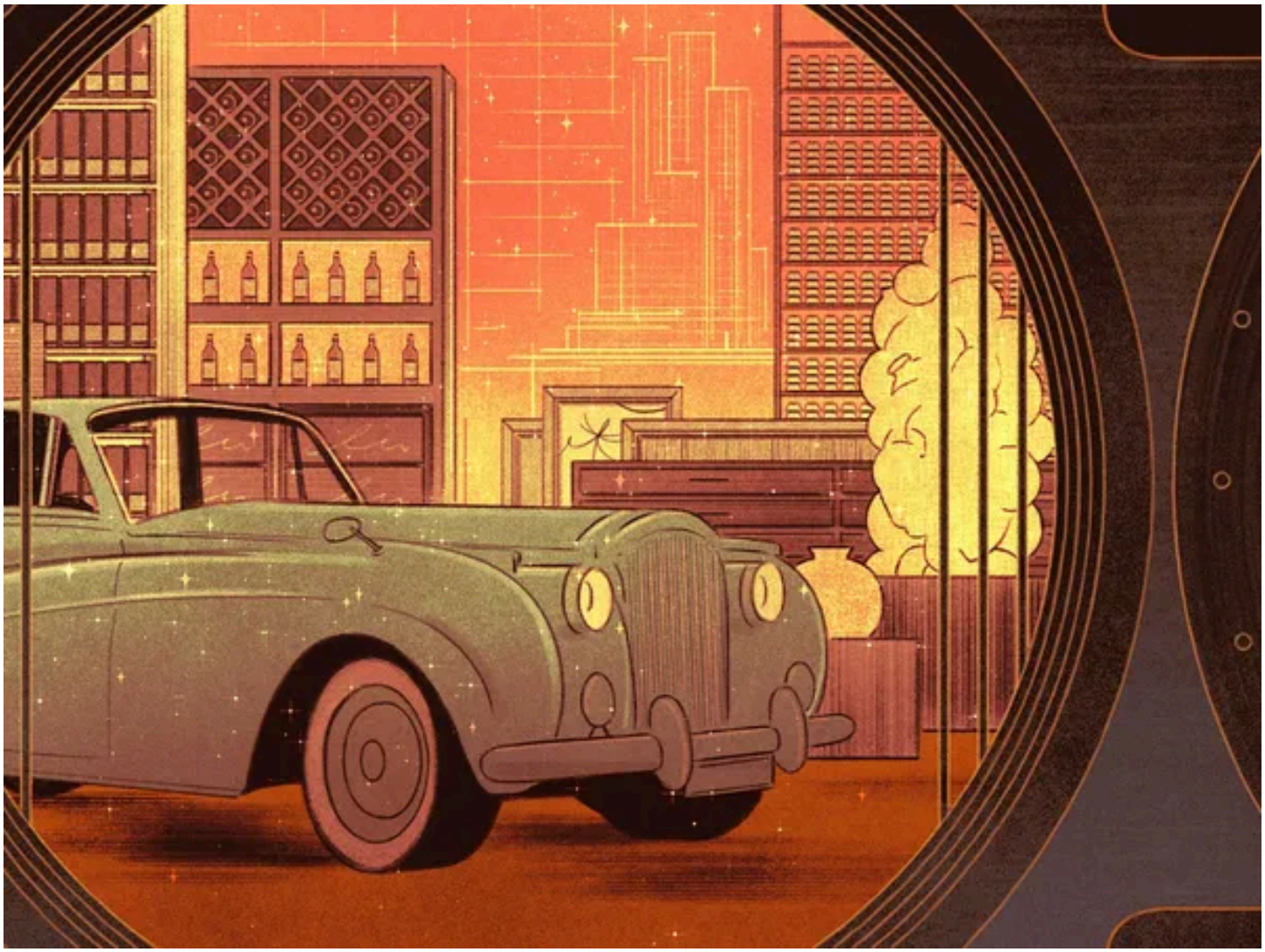
Where to Invest $100,000: Energy, Agriculture and Digital Payments

by Paulina Cachero



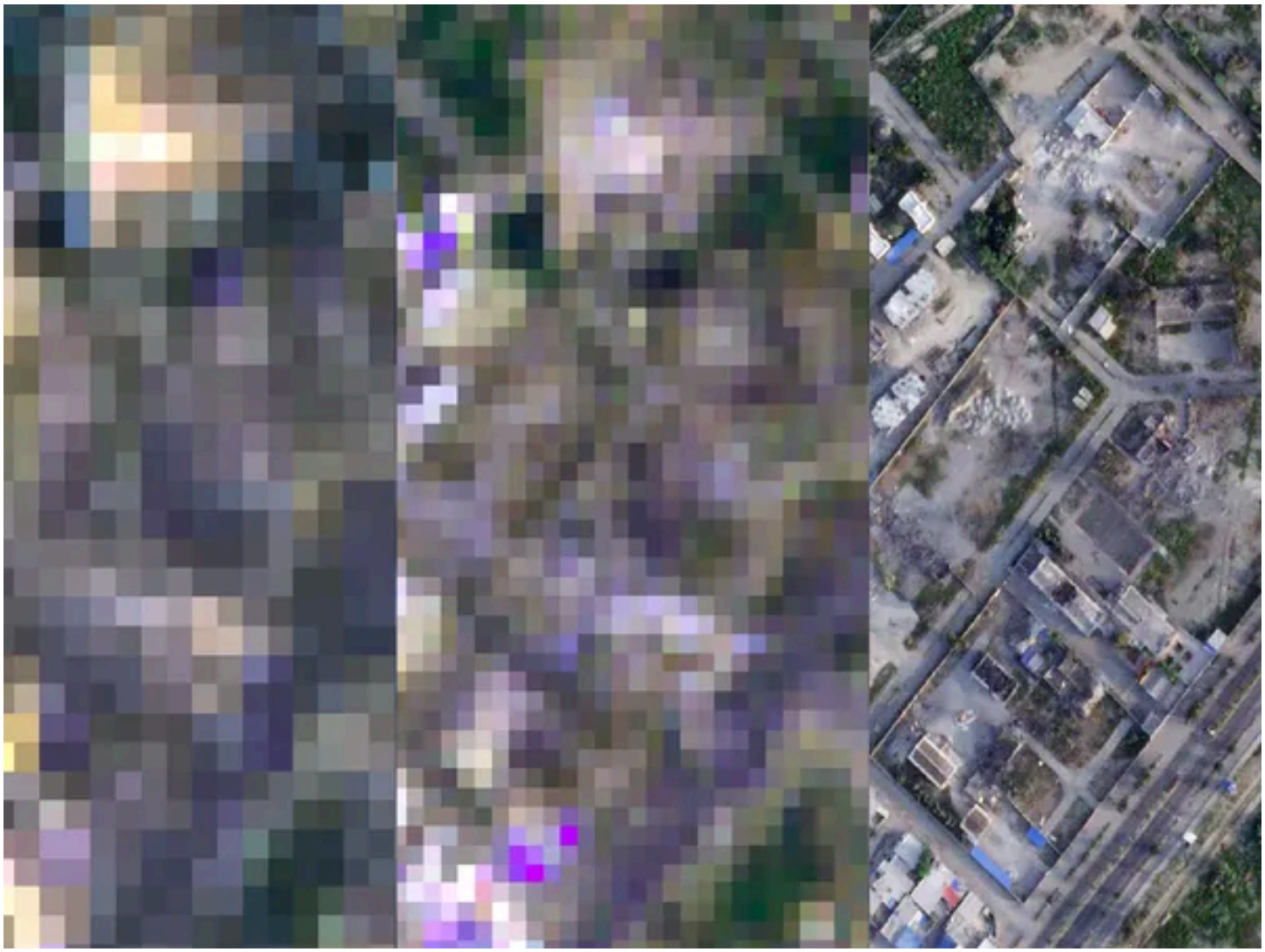
What Mohammed bin Salman Fears Most From the Iran War

by Mishal Husain



Where to Invest $1 Million: Critical Minerals, Quality Stocks, Gold — and Red Wine

by Suzanne Woolley



How US Data Restrictions in Iran Are Reshaping the Satellite Imagery Industry

by Krishna Karra

Terms of Service Do Not Sell or Share My Personal Information Trademarks Privacy Policy

Careers Advertise Ad Choices Help

©2026 Bloomberg L.P. All Rights Reserved.