May 2019 Issue

Real estate's surveillance state

As the industry ushers in new tech advancements — from people-tracking to facial recognition — fears about privacy and Big Brother-like tactics are taking hold

By Rich Bockmann | May 01, 2019 01:00PM

The Edge in Amsterdam is widely considered the smartest building in the world.

Since the 15-story office property opened four years ago, its 28,000 sensors have collected roughly 55 terabytes of data on everything from the air's CO2 levels to workers' daily coffee orders. If that information were stored as music files, it would play continuously for more than 100 years.

And the more info the glass-encased building collects, the smarter it gets.

"We think of it as a computer with a roof on it," Jan-Hein Lakeman, executive managing director of developer Edge Technologies' U.S. operations, told *The Real Deal*.

The 22-year-old firm, based in Amsterdam, recently co-developed a 325,000-square-foot office building in New Jersey as Unilever's North American headquarters — which also uses a cloud-based computing system and workplace sensors. And this year, Edge Technologies plans to announce its first project in New York City. Lakeman said the company is now looking at sites for either a ground-up development or an existing building that it can "Edge-ify."

The real estate industry — which has a reputation for being slow to adopt new technologies — is in the early stages of a tech transformation fueled, in part, by consumers wanting to be more connected. From landlords to property managers, companies across the industry are spending billions to outfit offices, residential properties and retail with new smart gadgets. And the information those devices are collecting is getting stored and Ping-Ponged across the web at increasingly faster speeds.

> **"I do understand the paranoia that exists. Right now, it's new. But I would bet money that in 10 years it is going to be so commonplace all over the world."**
>
> **ROBERT NELSON,** NELSON MANAGEMENT

Meanwhile, the latest advancements in artificial intelligence allow buildings to process and "think" about the information they've collected and make operational adjustments.

But as real estate players in New York and beyond look to roll out new technologies like facial scanning and geolocation tracking, it's stoking new anxieties over science fiction levels of surveillance. On top of privacy concerns, smart buildings raise the risk of cyberhacks and data breaches, critics say.

In this environment, lawmakers around the globe are pushing to impose tighter regulations. The European Union last year implemented the world's strictest data privacy law, and similar legislation will go into effect in California next year.

"The question is, where is that line between privacy and convenience: How much Big Brother am I afraid of?" said Brian Zrimsek, a principal at MRI Software, a real estate management and investment software provider.

In New York, those anxieties were thrust into the public spotlight in March, when it was revealed that Brooklyn landlord Nelson Management plans to install facial recognition technology at several of its rent-stabilized buildings around the city. Tenants at Nelson's Atlantic Plaza Towers

complex in Brownsville filed an objection to the plan, citing a potential for violations of privacy and civil liberties.

Nelson Management's Atlantic Plaza Towers

The company's president, Robert Nelson, said the technology will help the landlord fulfill one of its most important responsibilities: providing for the safety of his tenants.

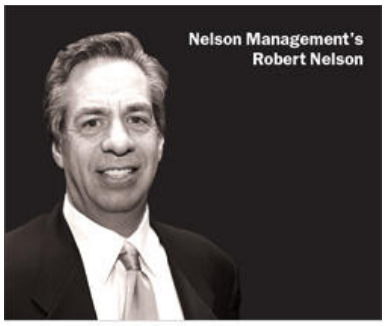
But he also acknowledged his tenants' concerns.

"I do understand the paranoia that exists," he said. "Right now, it's new. But I would bet money that in 10 years it is going to be so commonplace all over the world."

Tracking tenants

The biggest surveillance case study is unfolding right on Manhattan's Far West Side at Hudson Yards.

The Related Companies' mega-development collects so much data from residents, workers and tourists that it bills itself as the country's first "quantified community."



The $25 billion megaproject's office towers feature a biometric scanning technology called Pass that uses handprints to give tenants access. The 16-building site will also have a content management system including 30 kiosks with touch screens that can be used for things like booking a restaurant or buying tickets to the "Vessel." But those kiosks will also be siphoning information from visitors, including their browser histories.

In March, Related saw public blowback over the terms and conditions for its Vessel sculpture, which stated that all photos taken by visitors belonged to Related, giving the firm the right to license and sell them in perpetuity. The developer walked that policy back following the outcry.

Jay Cross, who heads Related Hudson Yards, told *TRD* in March that he and his associates are still deciding how they'll use all of the data they're collecting. While Related has no plans to sell its user information for the time being, Cross signaled the company could do so in the future.

"We can do … what we want with our data; we're not averse to using it to help the city map the West Side," he noted.

Meanwhile, global brokerages like CBRE and JLL are investing heavily in new technologies that track and analyze what goes on inside office and retail spaces. CBRE, for example, buys geolocation data that other companies collect from mobile phones, and uses it to show retailers info about who visits particular locations. And co-working and co-living companies are "programming" properties for tenants, while a growing number of smart apartments are hitting the market.

"For a very long time, people have been promised the 'Minority Report'-esque level of technology in buildings," said Chase Garbarino, CEO of the property tech firm HqO.

Garbarino, whose startup makes an app that commercial tenants can use to book conference rooms and schedule visitor access, among other things, said the smart-building evolution comes down to how many devices feed information to the cloud. "A lot of these pieces are coming online now," he added.

All of the data from the Edge in Amsterdam, for example, is fed into a Microsoft cloud platform, which tracks the movements and routines of the people inside by using an app on their phones.

By 2022, 4 billion devices linked to the "internet of things" (IoT) — everyday gadgets that are increasingly becoming connected online — are expected to be in homes worldwide, while more than 3 billion are expected to be in office buildings, according to the smart-building research firm Memoori.

The Vessel at Hudson Yards

That disruption hasn't come without its share of apprehension.

In Canada, for example, mall owner Cadillac Fairview stopped using facial recognition scanners at two of its Calgary shopping centers last summer after Reddit users discovered the technology could approximate visitors' ages and genders. Under Canadian privacy laws, visitors have the right to request that Cadillac Fairview stop collecting their data. But some argue that wasn't really an option, since the mall owner hadn't disclosed it was using the technology.

The company, which is owned by the Ontario Teachers' Pension Plan, is currently under investigation by Canada's privacy commissioner.

Similarly, critics of Google affiliate Sidewalk Labs — Daniel Doctoroff's smart-cities planning firm — launched a #BlockSidewalk campaign protesting its surveillance at the 12-acre development known as Quayside, which the company is helping to build in Toronto.

Jathan Sadowski, a researcher at the University of Sydney who studies smart systems, said buildings, and even entire cities, are becoming more like Facebook and Google when it comes to

pushing the boundaries about how much and what kind of personal information they have on people.

“I wouldn’t be surprised if we’re witnessing the very beginnings of something that becomes the new normal,” Sadowski said. “The built environment having terms of service agreements.”

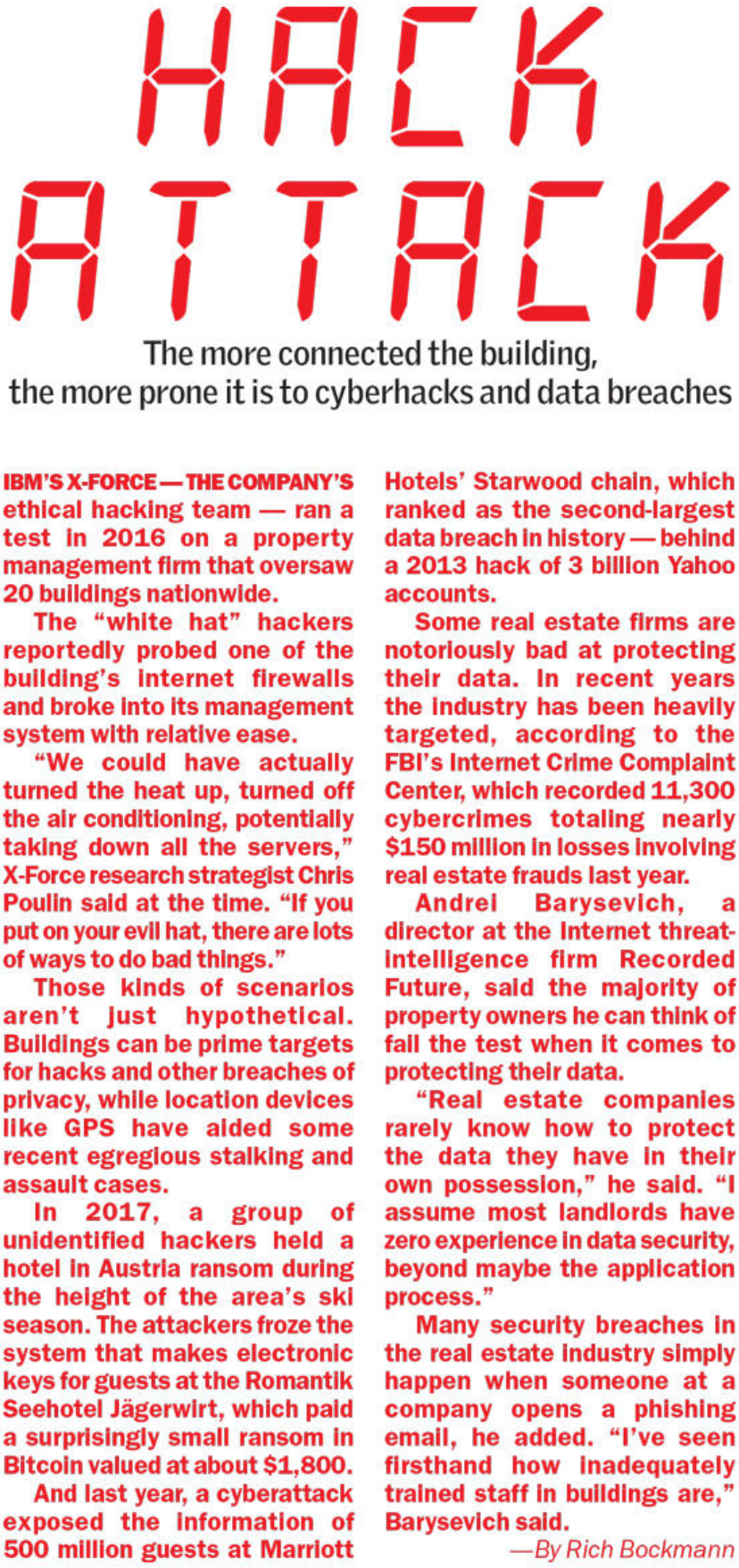
WeWatch

Nothing encapsulates the We Company’s casual culture and lofty ideas about the power of data quite like the T-shirt its executive David Fano wears with the motto “bldgs = data” printed on it. Fano — who trademarked the logo at a real estate consulting firm he launched before joining WeWork in 2015 — is one of the biggest proponents of optimizing work and living spaces by quantifying and analyzing occupants’ routines.

The info that WeWork compiles on its members includes their intellectual property such as trademarks and logos, companies and job titles, social media screen names, online calendars and passwords, relationships to emergency contacts and even their favorite foods and snacks. The company’s surveillance also includes requests made through Amazon Echo as well as communications on Slack and email.

And as Manhattan’s largest private office tenant, the co-working giant is in a unique position to test its theories.

“We’ve kind of got this big petri dish of people working in different ways with each other across the globe and different time zones,” Fano said during a conference at the University of Pennsylvania’s Wharton School last spring. “It’s a physical social network, and people are always together all the time.”



HACK ATTACK

The more connected the building, the more prone it is to cyberhacks and data breaches

IBM'S X-FORCE — THE COMPANY'S ethical hacking team — ran a test in 2016 on a property management firm that oversaw 20 buildings nationwide.

The "white hat" hackers reportedly probed one of the building's internet firewalls and broke into its management system with relative ease.

"We could have actually turned the heat up, turned off the air conditioning, potentially taking down all the servers," X-Force research strategist Chris Poulin said at the time. "If you put on your evil hat, there are lots of ways to do bad things."

Those kinds of scenarios aren't just hypothetical. Buildings can be prime targets for hacks and other breaches of privacy, while location devices like GPS have aided some recent egregious stalking and assault cases.

In 2017, a group of unidentified hackers held a hotel in Austria ransom during the height of the area's ski season. The attackers froze the system that makes electronic keys for guests at the Romantik Seehotel Jägerwirt, which paid a surprisingly small ransom in Bitcoin valued at about $1,800.

And last year, a cyberattack exposed the information of 500 million guests at Marriott Hotels' Starwood chain, which ranked as the second-largest data breach in history — behind a 2013 hack of 3 billion Yahoo accounts.

Some real estate firms are notoriously bad at protecting their data. In recent years the industry has been heavily targeted, according to the FBI's Internet Crime Complaint Center, which recorded 11,300 cybercrimes totaling nearly $150 million in losses involving real estate frauds last year.

Andrei Barysevich, a director at the internet threat-intelligence firm Recorded Future, said the majority of property owners he can think of fail the test when it comes to protecting their data.

"Real estate companies rarely know how to protect the data they have in their own possession," he said. "I assume most landlords have zero experience in data security, beyond maybe the application process."

Many security breaches in the real estate industry simply happen when someone at a company opens a phishing email, he added. "I've seen firsthand how inadequately trained staff in buildings are," Barysevich said.

—By Rich Bockmann

The SoftBank-backed company, which late last month filed preliminary paperwork for a long-anticipated IPO, does indeed resemble a social network — at least in terms of its privacy policy.

The membership agreement for 110 Wall Street, a WeLive co-living property, states that it collects extensive information from its members through their devices and their use of the space. By signing it, members agree to allow WeLive to use and share their personal data.

The We Company has built up a massive infrastructure to collect data on its more than 400,000 members. In February, for example, it acquired Euclid, a startup it describes as a "Google analytics for space" that gathers troves of info on people through their Wi-Fi connections. The company's WeWork arm is also looking into using facial recognition and workplace sensors that track things like motion, temperature and Bluetooth check-ins.

Bryan Murphy, CEO of the flex office space startup Breather, said he's seeing some members leave WeWork due, in part, to concerns about the company's privacy policies. Murphy acknowledged that Breather also collects a certain amount of data from its members, but said he has decided against using facial recognition and workplace sensors. And the company doesn't share its data with outside parties, he emphasized.

"That's actually part of our value proposition," Murphy said.

A spokesperson for the We Company declined to comment for this story. But in the past, company executives have said the information is aggregated and anonymized — a common rebuttal to privacy concerns.

The company also says the information helps improve its services. It does, however, reserve the right to share the data with other parties. While the identities of those parties are often masked in vague language, they generally include hired vendors and companies it partners with on transactions, including buying properties and other businesses.

> **"The minute you allow others into your buildings to retrieve that data ... if they're not sharing that with you and if it's going out the backdoor and being monetized, you're not doing your job."**
>
> **JOHN GILBERT,** RUDIN MANAGEMENT

Stacy-Ann Elvy, a New York Law School professor who studies privacy and emerging technologies, said that kind of language comes with a big loophole.

"The company has the control to determine who gets access, so I don't think promising not to sell the data is bulletproof in terms of fully protecting consumers," she noted. "If those provisions were as effective as [one would hope], we wouldn't have all these instances of companies selling our data to different parties."

Decoding data

Many of the real estate players who collect and use this kind of data claim they're looking only at big-picture trends, not at specific people. But many studies show that data can be decoded — or deanonymized, in surveillance-speak — and used to identify real people.

In a Massachusetts Institute of Technology study published in December, researchers took an "anonymized" set of location stamps from mobile phone logs in Singapore and matched it up with riders' location stamps from the city's transit system. The researchers estimated they could positively identify 95 percent of the study's participants with 11 weeks' worth of data.

"I was at Sentosa Island in Singapore two days ago, came to the Dubai airport yesterday, and am on Jumeirah Beach in Dubai today. It's highly unlikely another person's trajectory looks exactly the same," MIT Prof. Carlo Ratti, one of the study's authors, wrote.

"In short, if someone has my anonymized credit card information, and perhaps my open location data from Twitter, they could then deanonymize my credit card data," he added.

Studies have also shown that most people don't read privacy policies, and even if they did, it would take months to understand them. That's not to mention that most people have no choice but to accept that reality — unless they want to forgo having a phone, email account, social media presence or office job.

By now, most people understand that visiting a website or downloading a free app comes at the price of handing over their information.

There's a secretive industry built around the buying and selling of personal data, and the information from buildings is particularly useful to that market.

Data brokers like Oracle, Experian, Equifax and a web of lesser-known names buy and sell personal data that's used for everything from marketing to checking a renter's credit history.

But while websites can track online habits and phones can monitor locations, both have data limitations. Mobile phone tracking, for example, can tell when someone walks into a building. But it's not very good at determining if the phone is in a ground-floor restaurant or the observation deck of a skyscraper.

Embedding these technologies in the buildings themselves can help

fill in those gaps and turn people's everyday actions into data points.

"What's different is you get an inside window into what people are doing offline," New York Law School's Elvy said.

"If you were walking into the common area of your building, typically that's not viewed as data anyone would collect," she added. "But now it is, because they know what time certain individuals are opening the door, and there's a detailed record of that."

The chunk of Marriott Hotels' Starwood customers whose personal data was potentially compromised in last year's cyberattack — the second-largest in history

100M+

The number of Alexa devices Amazon has sold around the world, according to the e-commerce giant

95%

The portion of Singapore public transit riders MIT researchers estimate they can identify using 11 weeks' worth of "anonymized" cell phone data

Greater good?

Of course, the benefits go beyond bigger profits and greater control for individual firms. Smarter buildings can also potentially help save the planet.

Nearly 40 percent of the country's carbon emissions comes from buildings, according to the Washington, D.C.-based independent nonprofit Environmental and Energy Study Institute. And just last month, the New York City Council passed sweeping legislation requiring large buildings to be retrofitted to reduce fossil fuel consumption by 2030.

With the projected costs for New York landlords to come into compliance exceeding $4 billion, experts in the tech world say data-collecting sensors and AI — which can collect untold numbers of data points to spot places where buildings are wasting energy — can go a long way.

"It's very important for [property managers] to not waste their time looking for issues but dedicate their time out in the field to preventing and solving those issues," said Luca Tausel, of IBM's Watson unit, which creates the AI used in many smart buildings.

In 2016, the family-run real estate firm Rudin Management launched its own tech startup, Prescriptive Data, which uses a cloud-based operating system in 17 of the developer's New York properties to more efficiently manage their water and electricity use, among other building systems. Last year, those properties recorded a 44 percent reduction in carbon emissions — more than the 40 percent reduction the City Council's law mandates over the next decade.

Rudin's technology chief, John Gilbert, said Prescriptive Data anonymizes building information. And in the cases where it's put to use in buildings run by other landlords, he said, the data belongs to each property owner rather than to Rudin's tech company.

More broadly, Gilbert noted that there are lots of lessons property owners can learn from Silicon

Valley's privacy headaches.

"I think the Facebook lessons are hugely important," he said. "The minute you allow others into your buildings to retrieve that data … if they're not sharing that with you and if it's going out the backdoor and being monetized, you're not doing your job."

At the same time, properties are increasingly adding devices that interact with buildings' occupants.

The Stanwix in Bushwick, for example, bills itself as the smartest rental in Brooklyn.

The 130-unit building, owned by JCS Realty, has a Control4 automation system that tenants can access through a wall panel or a mobile app to do things like alter the lighting and adjust blinds. Tenants can also use smartphones remotely to operate door locks and create a log of every time the lock is used — and who used it.

The Stanwix uses a management system created by the cloud-based platform BuildingLink, and the tech is all linked to an Amazon Alexa provided by the landlord. A representative for JCS did not respond to requests for comment.

Ari Teman, whose company makes video intercoms and smart locks, said tenants often want a certain level of surveillance.

"Surveillance can make you feel safe," added Teman, who said his technology is used in about 1,000 residential buildings in New York City. "When I'm living in a building, I want the package area and the lobby entrances areas to be recorded and for cameras to be visible."

Teman added, however, that data collection can certainly cross a line.

"If you want to take that data and sell it to some big company to tell about my love life, I find that creepy," he said.

The Amazon effect

In New York and other major cities, rentals, condos and single-family homes are linking to devices made by "Big Tech" companies at an increasing rate, reports show.

Amazon announced in January that it had sold more than 100 million Alexa products around the globe, and an RBC analyst estimated late last year that Google had sold more than 52 million home devices worldwide.

Tech behemoths like Amazon, Microsoft and IBM also run the cloud systems that many smart buildings use. Virtually all of those companies have reputations for pushing the privacy envelope — and, in turn, prompting laws to more carefully regulate the space.

"Lots of companies are now supplying what you will see in your apartment, in your home, on the

wall," said Gordon Feller, co-founder of the smart-cities summit Meeting of the Minds. "The goal is to deliver advertising to the end user, which is going to be a shock to a lot of people when they realize that."

There's also just the looming fear that these devices are recording conversations people are having in their own homes. And there have been documented cases suggesting that it happens when signals cross.

A family in Portland, Oregon, for instance, caught its Amazon Echo last year haphazardly recording one of their conversations, which it sent to one of their phone contacts, according to news reports.

"It's only natural that the likelihood of these types of incidents happening is only going to increase as the tech becomes more widespread," said attorney Kavon Adli, a partner at the Internet Law Group based in Los Angeles. "New companies are coming on the scene pretty regularly, and there's no universal fix for these kinds of problems."

Big Brother business

It's not just rental landlords, shared-space providers and property managers buying into the smart-building market. Large commercial brokerages, construction firms and megadevelopers are investing billions in building analytics and other intelligent services.

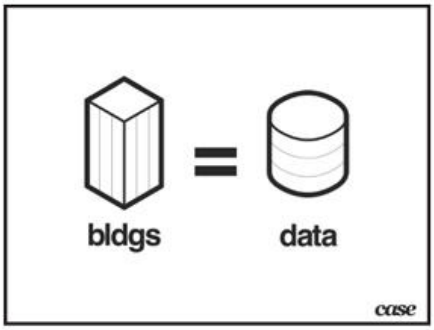
In real estate, the retail sector was among the first to adopt so-called alternative data. Landlords and commercial brokers purchased the people-tracking data from mobile phone companies and then provided retailers with intel on shopper demographics and foot traffic.

Big real estate firms are now creating their own intelligent technologies.

CBRE, for example, launched a workplace app last year that uses artificial intelligence to learn office tenants' patterns and make recommendations for them.

Connecticut-based Triax Technologies, meanwhile, created a wearable device that uses an accelerometer and gyroscope to monitor a construction worker's gait. If the hard hat gets drunk during lunch and stumbles back to the jobsite, the device will detect the unusual movement and report it to the worksite's superintendent, Triax claims.

Many argue that tech users and tenants are willing to trade some privacy for convenience. And companies face reputational risks if they betray customers' trust.



David Fano's trademarked logo

"If AT&T is monitoring your cell phone service and using data to figure out what they can do to create a better experience so that you have less dropped calls or whatever, that's kind of okay," said K.P. Reddy of Shadow Ventures, an Atlanta-based venture capital firm focused on the proptech industry. Though selling that info isn't illegal, it's "the big no-no," Reddy added.

Most real estate players using Big Data say they're gathering info to provide better services and don't sell that data to third parties, including advertisers.

But there are plenty of examples outside of real estate where companies have crossed the line.

Verizon was caught last year selling its customers' locations to a prison phone company — which corrections officers used to find out, without getting warrants, who inmates were calling. In the wake of that revelation, Verizon, AT&T and Sprint said they would all stop sharing information with certain third parties.

And plenty of questions remain about who the data belongs to — the manufacturer of the devices, the building manager or the property owner. That's led to other questions, including who the data stays with when a property sells.

Even when a company collects the data, it could change hands. In bankruptcies, for example, data can be sold off as an asset. A biometrics payment company called Pay by Touch filed for bankruptcy in 2007, and among its holdings was a database of 2 million fingerprints from people who bought gas and groceries using the technology. More recently, the IoT company Filip Technologies — which designed a smart locator for children so their families could stay in touch — filed for bankruptcy in 2016, selling off data about the parents and children who used its devices.

While that largely stayed under the radar, other privacy battles are brewing.

Airbnb, for one, sued the city of New York last year after it passed a law requiring the company to hand over data on its hosts, including their names, addresses and number of days they rented their homes.

Airbnb argued there was no way to know what the city would do with the data. In January, a federal judge sided with the company, blocking the law from taking effect.

Information the city sought includes "personal data in which Airbnb has a reasonable

expectation of privacy," and most hotels "would balk at any suggestion that their patrons' privacy could be invaded in such a manner," the company's complaint read.

A spokesperson for Airbnb declined to comment.

Global backlash

Just a few weeks after Mark Zuckerberg testified in front of Congress in April 2018 about Facebook's privacy policies, Europe took a major step forward on regulating data privacy.

The next month, the European Union's General Data Protection Regulation — the toughest and most comprehensive legislation of its kind in the world — went into effect.

Among its many rules, the law requires companies to get consent from people in the EU to process their data and gives those individuals the right to withdraw that consent at any time (see sidebar). It also requires companies that collect data to put security protections in place and gives people the right to have their data erased within 30 days.

WILL GDPR RAISE THE BAR?

A look at Europe's sweeping privacy law and what it means for global real estate firms and other businesses

SINCE EUROPE'S DATA PROTECTION law went into effect in May 2018, regulators have received reports of more than 59,000 personal data breaches, a February study from the global law firm DLA Piper found.

The General Data Protection Regulation, or GDPR, requires organizations that are based or do business in the European Union to report privacy breaches within 72 hours, among several other mandates. While figures are scarce on which kinds of companies have been impacted by the new law, experts say it has serious implications for all businesses that collect personal data, including real estate firms.

"This is a complete overhaul of EU data protection law, and it does make people nervous because we don't know exactly how certain things will be impacted," said Chloe Kite, an attorney at DLA Piper in London.

GDPR also impacts companies in the U.S. that deal with people in the EU. International players like the Blackstone Group already have GDPR notices on their sites. And many believe it's a matter of time before similar federal legislation works its way to the States.

But experts say it's still too early to tell exactly how regulators will apply Europe's sweeping law, and whether they'll look for high-profile cases to make examples of. According to the DLA Piper report, only 91 fines have been doled out since GDPR took effect — a low figure that indicates regulators may already be stretched thin.

In the meantime, companies have become compliant by mapping out what kinds of data they collect and how long they keep it. Patrick Wheeler, head of the intellectual property and data protection practice at the London-based law firm Collyer Bristow, said one of the key principles to consider is the law's requirement of data minimization. That rule requires companies to keep only as much data as they need for business purposes, and to be ready to spell out what those purposes are.

"Indeed, one of the questions is, if you want to reduce the risk that you face in relation to data breaches, you should really ask yourself the question, 'Do I need to have all this data?'" Wheeler said.

—By Rich Bockmann

Many believe that similar federal legislation will eventually work its way to the U.S. But for now, cities and states are implementing their own laws.

California passed a consumer privacy act last year, which goes into effect in 2020. That initiative — which requires companies to disclose how they collect data and what they do with it — was actually initiated by San Francisco real estate developer Alastair Mactaggart, who became concerned about Big Tech's surveillance.

In New York state, there's a patchwork of privacy laws, but nothing as far-reaching.

State Sen. Brad Hoylman is pushing his "right to know" legislation that would let consumers find out what kind of data companies are collecting and how it's being used, but it stops short of banning companies from selling personal information.

And last fall, City Council member Ritchie Torres introduced a bill to regulate facial recognition technology, which he likened to a secret search. The bill calls for a fine of $500 every day a company fails to disclose its use of biometric scanning tech and gives people the right to sue for damages of up to $5,000.

"I just believe as a matter of principle that no business has a right to search or invade your privacy without your knowledge or consent," Torres said. "It's the lack of transparency that worries me the most."

Fear factors

Of course, there's always a sense of unease when new technologies come into play.

Some argue that backlash against real estate's data harvesting could be just be an unfounded fear of the unknown.

In many cases, both landlords and tech companies are compiling as much data as they can without any real idea of how they're going to use it. The belief is that the data will have some value in the future.

"In some ways, it's potentially more worrisome that the data's being collected, and we don't know what for," said Desiree Fields, a professor of urban and economic geography at the University of Sheffield in England. "Particularly in the U.S., where there's so little data protection, we're right to be concerned about that."

Some also note that this kind of data collection is in its infancy in real estate and say that as it gets implemented on a larger scale, it is likely to improve.

"We are like 10 years out from even 30 percent adoption of this kind of technology," said Ash Zandieh, founder of the proptech research firm RE:Tech.

HqO's Garbarino said all this new technology in buildings has the potential to do great things, but he also recognized the dangers they pose.

"It's naïve to think technologies are inherently good," he said.

Garbarino added that now, when the rules are being written, is the time to make sure it's done right.

"The real estate industry has an opportunity to be very proactive to make sure they're not misusing any of this data," he said.