GLOBAL

The Tech Site That Took On China's Surveillance State

How did a trade publisher in Pennsylvania become a principal source of investigative journalism on the repressive apparatus Beijing uses against the Uyghurs?

By Timothy McLaughlin

Tyler Comrie / The Atlantic

SEPTEMBER 30, 2022

SHARE

Updated at 2:10 p.m. ET on September 30, 2022

BETHLEHEM, Pa.—Behind Heights Market & Deli ("Home of the Hoagie") and next to Finishers Mixed Martial Arts gym, in a neighborhood of tidy lawns adorned with reflective gazing balls, sits a mundane warehouse that is the headquarters of an obscure news organization with an equally mundane name: Internet Protocol Video Market. The nondescript location gives little clue about what kind of journalistic enterprise goes on here.

IPVM's office has no newsroom with reporters clacking on keyboards and TVs playing cable news. Instead, technicians run surveillance cameras and other security equipment through a litany of tests. Some journalist staff undertake more traditional reportorial tasks, digging through company filings and financial documents for reports that appear on IPVM's website.

For most of its 14 years of publishing, the company existed as a niche, industry-focused outlet, read by professionals and technicians who generally worked in the field of commercial surveillance. In recent years, though, IPVM has delivered a string of highly impressive scoops, many in collaboration with major news organizations such as *The New York Times*, *The Wall Street Journal*, and the *Los Angeles Times*, that have revealed alarming and sinister aspects of what Chinese surveillance companies have been up to. A December 2020 report by *The Washington Post* based on a document unearthed by IPVM detailed efforts by the Chinese tech giant Huawei to develop a face-scanning system that could trigger a "Uyghur alarm"—referring to the mainly Muslim ethnic group of northwestern China that has faced heavy state repression. The article prompted a European executive to resign from Huawei shortly after, and in February 2021 to speak out about the company's technology.

The same month, the *Los Angeles Times* published a report based on a user guide found by IPVM in which the Chinese firm Dahua claimed that its camera technology could identify Uyghurs and automatically alert authorities when it did so. The revelation prompted a group of U.S. senators to write to Amazon demanding to know why the company had signed a multimillion-dollar deal with Dahua. Both the bipartisan Congressional-Executive

Commission on China and the U.S. State Department have noted IPVM's work in their reports on China.

This record of breaking important stories has made IPVM a closely read publication among not just people interested in surveillance technology but those who want to understand Beijing's geopolitical ambitions, as well as the deeply strained relations between the United States and China, arguably the world's most consequential bilateral relationship.

Read: Seeking sanctuary in the old empire

IPVM was founded in 2008 by John Honovich, who was then a disaffected exile from the surveillance industry after a couple of unpleasant experiences at security-technology

RECOMMENDED READING

firms that overpromised and under-delivered. In a recent interview, Honovich, now 46, told me he had been taken aback by the number of "deceptions and lies that were so commonplace," which involved a lot of "fake-it-'til-you-make-it–type stuff." These experiences made him realize that "being unethical is one of the greatest sources of competitive advantage."

How History Classes Helped Create a 'Post-Truth' America

ALIA WONG

The Vindication of Cheese, Butter, and Full-Fat Milk

JAMES HAMBLIN

Dads Prefer Sons, Moms Prefer Daughters

JOE PINSKER

Honovich holds trade publications in low regard. Many, he believes, have been "bought" by advertisers who hold sway over reviews and content. To avoid this, he said, he started IPVM with his own money and refused to run ads. At first, the site focused on aggregating news about the surveillance-and-security-technology industry. Later, he added commentary and analysis, and before long he started running his own, rudimentary tests of camera equipment.

"He was shooting stuff in parking lots and out of his balcony door," Ethan Ace, one of the company's first employees, told me. "But nobody else was doing any independent testing at all." Today, the site employs about 25 people and has more than 15,000 subscribers.

Ace is now the head of testing at IPVM, whose facilities have evolved from "the back of my Volvo in a field" to a cavernous 12,000-square-foot hall with lockers holding some 600 cameras that have been tested and broken down. During a visit in August, I noticed a collection of Bowie knives on a set of shelves. Don Maye, IPVM's head of operations, explained that these were for testing the effectiveness of AI scanning technology whose makers say it can detect concealed weapons. Companies marketing such tools have seen a surge of interest since May's school shooting in Uvalde, Texas. Ace and Maye were highly skeptical of the claims made for the technology.

Read: China's surveillance state should scare everyone

Ace, who describes himself as "the proudest card-carrying ACLU member in the security industry," showed me another bay where a thermal camera made by a Chinese firm was being tested. This was an example of technology that proliferated during the coronavirus pandemic, in what Ace called the "fever-camera craze."

Calamitous episodes, such as mass shootings and terrorist attacks, create booms for the security industry. COVID-19 was no exception. "We are an industry that is specifically marketing towards people's fears," Ace said. "That is the nature of it."

A nearby screen displayed our images and supposed body temperatures. When Ace wore his eyeglasses, everything was fine. When he removed them, an alarm sounded to indicate that his temperature was too high. This was only an impromptu experiment, but it showed how unreliable the readings can be. (Ace was a co-author, along with other IPVM employees, of a March 2021 paper in the *Journal of Biomedical Optics* describing how thermal-camera manufacturers can manipulate readings to compensate for imprecise measurements and thus undercut the medical usefulness of the technology.)

Honovich remains IPVM's public face, which has made him a target of anonymous blogs and Twitter accounts. Some accuse him of being a self-promoting gadfly or a bully who uses IPVM to besmirch companies he dislikes. Honovich occasionally tangles with his detractors in IPVM's comment section and on LinkedIn.

"He obviously pisses people off," Gordon Haupt, who worked with Honovich in the early 2000s and is now a software engineer for Spotify, told me. "But it is because he is trying to tell the truth."

According to Honovich, the site made no conscious decision to concentrate on China. If there was a "bad actor" that IPVM set out to cover, "it was Silicon Valley, not the PRC," he said. But as Chinese firms made inroads into the U.S. market, offering cheap hardware that was upgrading all the time, the site couldn't ignore them. "The industry coming out of China was a lot bigger than we realized," Ace told me.

This was something he grasped only when he attended the enormous China Public Security Expo trade show in 2015. When he visited the offices of companies such as Hikvision, the world's largest maker of surveillance equipment, Ace glimpsed a piece of what Josh Chin and Liza Lin of *The Wall Street Journal* have described as one of Chinese President Xi Jinping's "grandest ambitions"—"the creation of a new type of modern government, powered by data and mass digital surveillance, that can rival democracy globally."

As IPVM-enabled investigative journalism has helped bring to light, some of the most disturbing and dystopian elements of this plan have played out in Xinjiang, the region where Uyghurs and members of other largely Muslim groups face a "consistent pattern of invasive electronic surveillance," in the words of a United Nations report published last month. China's actions in the region, the UN concluded, "may constitute international crimes, in particular crimes against humanity."

IPVM's focus on Chinese surveillance technology has come as tensions—military, economic, and ideological—between the U.S. and China have been growing. Besides the human-rights situation in Xinjiang, Beijing's more belligerent approach to Taiwan, which it regards as part of China despite the Chinese Communist Party's never having controlled it, and the crushing of Hong Kong's prodemocracy movement have made relations between the two powers difficult. In Washington, a distrust of Beijing and the desire to confront China more aggressively are rare examples of bipartisan consensus.

Read: 'I never thought China could ever be this dark'

"Every single business relationship in China deserves serious scrutiny. That is especially true when it comes to technology," Marco Rubio, the Republican senator from Florida, who has made this issue a personal cause, told me in an email. "Research from firms like IPVM is critical to helping the media, policy makers, and the American people understand the threat posed by the Chinese Communist Party and the extent some companies will go to bypass American laws." Hikvision and Dahua were blacklisted by the U.S. Department of Commerce in 2019, over Beijing's treatment of the Uyghurs and other minorities.

Xinjiang has not been the only focus of IPVM's investigative work. Documents it procured formed the basis of a 2021 *Reuters* report about how the authorities in Henan, one of China's largest provinces, had commissioned a surveillance system that they hoped could track journalists and international students as well as other "suspicious people." This past June, an investigation by *The New York Times* of how China uses surveillance to reinforce social and political control drew partly on records obtained by IPVM.

Beijing has in recent years restricted the work of foreign journalists, often under the guise of public health as it continues to pursue a zero-COVID policy, and curtailed the number of reporters who can work on the ground. Enterprising researchers have instead scoured the internet, where social-media posts, satellite images, and technical documents can provide a new way into one of the world's most watched stories. Even this is becoming a challenge.

"That information is still out there," Dahlia Peterson, a research analyst at Georgetown University's Center for Security and Emerging Technology who

focuses on China, told me, "but it is increasingly becoming a cat-and-mouse–type situation, where they are throwing up more technical barriers to the outside world."

IPVM continues to uphold Honovich's pledge of independence, and does not accept advertising, sponsorship, or consulting fees from manufacturers. "They could just be a company that runs objective tests on video-surveillance technology and leave it at that, and not get involved on the ethical side," Peterson said. "However, they very much take a moral stance against the abuse of surveillance technologies, and their contributions are invaluable."

That ethos was on full display last year when Conor Healy, who researches for IPVM the ways governments use surveillance technologies, traveled to Bishkek, the capital of Kyrgyzstan, to meet a man named Ovalbek Turdakun. A Christian Chinese national who had spent 10 months in a Xinjiang detention camp, Turdakun was able to travel to Kyrgyzstan but feared that he

could be deported back to China and face detention again. Healy, working with a friend and contacts in Kyrgyzstan, arranged for Turdakun and his family to fly to Turkey. Healy and his friend escorted them on the trip. From there the family was granted permission to travel to the U.S., and in April this year the Turdakuns arrived in Washington, D.C.

Read: The military-style surveillance technology being tested in American cities

Healy told me he didn't see IPVM as an advocacy organization, but Honovich endorsed Healy's action. "How much does it really help people in Xinjiang?" Healy said. "Probably not that much, which made me sad." Still, they agreed, it was the right thing to do.

The response from China to IPVM's work has been predictable. In 2018, IPVM's site was blocked in China, as many other Western news sites are. Earlier this year, *China Daily*, a state-backed newspaper, accused IPVM of being a "mass surveillance company." Another Chinese outlet amplified a tech-forum comment that likened the IPVM site to a blog run by former Secretary of State Mike Pompeo, who was sanctioned by China and continues to produce bombastic warnings about the country's threats.

Hikvision, though majority-owned by a Chinese state company, has responded to IPVM's reporting on its operations in that most D.C. of fashions: using its considerable lobbying presence in Washington to question IPVM's impartiality and credibility. In January, *Axios* reported that Hikvision had asked congressional ethics officials to investigate IPVM for potential lobbying-disclosure violations.

The pressure campaign seems unlikely to change IPVM's approach to journalism. To Honovich, you can't "both sides" China's use of surveillance technologies in Xinjiang, or any other topic with ethical implications. "I think it is very important that we clearly take ethical stands when ethical stands should be made," he told me. "I don't like this whole thing of 'Well, there are Nazis and not-Nazis, but I'm not going to take a stand between the two.'"

This article originally named IPVM's head of operations as Don Mayne and said that the company had been publishing for 18 years. In fact, its head of operations is Don Maye, and the company has been publishing for 14 years.