How Recent Admissions Prove That We are Living in George Orwell's 1984

By Russ Walker

March 2026

Rainey Center

There is No Privacy in the Modern Age of Cameras—Even Your Vacuum Can Be Hacked to Spy on You

In 1949, George Orwell warned the world about a future in which omnipresent surveillance, state-controlled information, and the weaponization of technology against citizens would define daily life. He called it 1984. He was off by a few decades. A cascade of recent, real-world admissions, from a Super Bowl commercial quietly unveiling a neighborhood surveillance network, to a hacked robot vacuum exposing 7,000 homes, to Israeli intelligence assassinating a head of state using an enemy nation's own camera grid, proves that Orwell's dystopia is no longer fiction. It is Tuesday. This paper examines how modern surveillance technology has evolved from a convenience into a weapon. How that weapon has already been used against foreign leaders, and why the Chinese Communist Party's mass surveillance export model now threatens its own architects. We are all living inside the telescreen.

The question is: who is watching?

The Smart Home is a Surveillance Network—With a Cute Face

The Ring Super Bowl Ad: Laundering Surveillance with Lost Puppies

On February 8, 2026, during Super Bowl LX, the most-watched television event in America, Amazon's Ring home security company aired a 30-second advertisement that, under the guise of finding lost pets, unveiled one of the most candid admissions of mass civilian surveillance infrastructure in corporate history.

The ad introduced “Search Party”, a feature that, when activated, deploys AI-powered object recognition across every participating outdoor Ring camera in a neighborhood to search for a missing dog. The commercial was designed to be heartwarming. The public reaction was anything but.

Key Facts and Admissions

When a pet owner posts a lost dog in the Ring app, nearby participating outdoor Ring cameras begin scanning their saved footage using AI, without any individual camera owner having to take action.[1]

The company has also rolled out Familiar Faces, which lets users register images of family and friends so their cameras can identify specific people, but limited to those the camera owner knows.[2]

The feature was turned on by default, requiring users to opt out, meaning millions of camera owners were participating without explicit knowledge or consent.[3]

Ring had inked deals with Flock Safety, a company supplying automated license-plate readers to law enforcement, and Axon Enterprises (makers of Tasers and body cameras), enabling police to access footage through a system critics called “a warrantless and anonymous community-request service.”[4]

---

1 GeekWire. (2026, Feb. 11). What Ring's "Search Party" actually does, and why its Super Bowl ad gave people the creeps. https://www.geekwire.com/2026/what-rings-search-party-actually-does-and-why-its-super-bowl-ad-gave-people-the-creeps/

2 GeekWire. (2026, Feb. 11). What Ring's "Search Party" actually does, and why its Super Bowl ad gave people the creeps. https://www.geekwire.com/2026/what-rings-search-party-actually-does-and-why-its-super-bowl-ad-gave-people-the-creeps/

3 GeekWire. (2026, Feb. 11). "Search Party raised privacy concerns when it launched last year, focusing in part on the fact that the feature is turned on by default in eligible cameras, requiring users to opt out." https://www.geekwire.com/2026/what-rings-search-party-actually-does-and-why-its-super-bowl-ad-gave-people-the-creeps/

4 Yahoo News / The Verge. (2026, Feb. 13). Why that Ring Super Bowl ad about finding your lost dog is creeping people out. Ring partnerships with Flock Safety and Axon Enterprises described. https://www.yahoo.com/news/us/article/why-that-ring-super-bowl-ad-about-finding-your-lost-dog-is-creeping-people-out-211647194.html

Local police departments were already searching Flock's camera network on behalf of U.S. Immigration and Customs Enforcement (ICE) and Customs and Border Protection (CBP), giving federal law enforcement side-door access to a tool it had no formal contract for.[5]

Surveillance expert with Electronic Freedom Foundation Matthew Guariglia warned: "It starts with searching for a brown dog, but means the tech is there for license plate reading, face recognition, searching for suspects by description."[6]

Amid public backlash, Ring was forced to cancel its Flock Safety integration, but the Search Party feature itself remains active and free to use.[7]

The critical takeaway is not the feature itself—it is what the ad revealed. Amazon openly confirmed, on the largest media stage in the country, that it has built a neighborhood-wide AI surveillance network inside American homes. The dog was just the cover story.

5 404 Media as cited in Yahoo News. (2026, Feb. 13). "Local police departments have already been searching Flock's camera network on behalf of U.S. Immigration and Customs Enforcement (ICE) and Customs and Border Protection (CBP), giving federal law enforcement side-door access to a tool that it currently does not have a formal contract for." https://www.yahoo.com/news/us/article/why-that-ring-super-bowl-ad-about-finding-your-lost-dog-is-creeping-people-out-211647194.html

6 Guariglia, M. [@mguariglia.bsky.social]. (2026, Feb. 9). [Post on Bluesky]. https://bsky.app/profile/did:plc:pxcupv4p27r73xgjw4s3lkqj/post/3mefgknsdac2u. As cited in: Zhang, S. "Super Bowl Ad for Ring Cameras Touted AI Surveillance Network." Truthout, Feb. 9, 2026. https://truthout.org/articles/super-bowl-ad-for-ring-cameras-touted-ai-surveillance-network/. Guariglia is Senior Policy Analyst, Electronic Frontier Foundation (EFF).

7 Variety. (2026, Feb. 13). Ring Cancels Flock Partnership After Backlash Over Super Bowl Ad. https://variety.com/2026/digital/news/amazon-ring-cancels-flock-partnership-super-bowl-ad-backlash-dog-finder-1236662108/

Your Robot Vacuum is Watching You: The DJI Romo Breach

If the Ring ad was a slow reveal, the DJI Romo story was a detonation. In February 2026, a software engineer named Sammy Azdoufal was attempting nothing more sinister than steering his robot vacuum with a PlayStation controller. What he accidentally discovered was a live window into nearly 7,000 private homes across 24 countries.

What Was Exposed

The same authentication token that gave Azdoufal access to his own DJI Romo also granted access to live camera feeds, microphone audio, real-time maps, and status data from 7,000 other devices.[8]

8 Popular Science. (2026, Feb. 21). Man accidentally gains control of 7,000 robot vacuums. DeGeurin, M. "The backend security bug effectively exposed an army of internet-connected robots that, in the wrong hands, could have turned into surveillance tools, all without their owners ever knowing." https://www.popsci.com/technology/robot-vacuum-army/

He could compile 2D floor plans of strangers' homes from the vacuum's mapping data, the precise kind of structural intelligence that would be invaluable to a burglar, a stalker, or a foreign intelligence service.[9]

IP address data revealed the approximate physical location of each device.[10]

DJI is a Chinese-owned company. The same company is already banned from U.S. government use due to national security concerns about data transmission to Chinese (CCP) servers.[11]

DJI patched the vulnerability. But the patch addresses one flaw in one device. The architecture that allowed it, cloud-dependent IoT devices storing sensitive data on remote servers remains intact across thousands of consumer products.[12]

The vacuum doesn't just clean your floor. It maps your home, records your conversations, and transmits that data to servers you will never see, controlled by people you will never meet—in countries that may not share your interests.

9 Popular Science. (2026, Feb. 21). Man accidentally gains control of 7,000 robot vacuums. "He also claims he could compile 2D floor plans of the homes the robots were operating in." https://www.popsci.com/technology/robot-vacuum-army/

10 Popular Science. (2026, Feb. 21). Man accidentally gains control of 7,000 robot vacuums. "A quick look at the robots' IP addresses also revealed their approximate locations." https://www.popsci.com/technology/robot-vacuum-army/

11 U.S. Department of Defense. (2021). Chinese Military Industrial Complex (CMIC) Annual Report. DJI listed as a company with ties to the Chinese military. As cited in Walker, R. Protecting Individual Privacy and Securing the Nation from 5th Generation Foreign Threats (2025). https://www.scmp.com/news/us/economy-trade-business/article/3329031/china-drone-maker-dji-appeals-inclusion-pentagons-chinese-military-companies-list

12 Popular Science. (2026, Feb. 21). Man accidentally gains control of 7,000 robot vacuums. DJI statement: "The issue was addressed through two updates, with an initial patch deployed on February 8 and a follow-up update completed on February 10." https://www.popsci.com/technology/robot-vacuum-army/


ring
Smart Security Outside.
A traditional alarm system that's anything but traditional.
Smart security at every home.

Surveillance as a Weapon of War—The Iran Precedent

On February 28, 2026, the United States and Israel launched a joint military strike against Iran. The opening blow was not a missile; it was an intelligence coup made possible by years of covert access to Iran's own surveillance camera network. The lesson for every nation and every citizen is unmistakable: surveillance cameras are not passive observers. In the right hands, they are targeting systems.

Israel Hacked Tehran's Traffic Cameras—For Years

According to reporting by the Financial Times, citing current and former Israeli intelligence officials, nearly all traffic cameras in

Tehran had been hacked by Israeli intelligence for years, with footage encrypted and transmitted to servers in Tel Aviv and southern Israel.[13]

Israeli intelligence used AI-powered algorithms, developed by IDF Unit 8200, to build detailed dossiers on Khamenei's security detail, including their home addresses, duty hours, driving routes, and which officials each guard was assigned to protect.[14]

One camera angle proved particularly decisive: it showed exactly where bodyguards parked their personal vehicles, allowing analysts to track patterns of movement in and out of Khamenei's compound on Pasteur Street.[15]

As one Israeli intelligence official stated: "We knew Tehran like we know Jerusalem. And when you know a place as well as you know the street you grew up on, you notice a single thing that is out of place."[16]

Simultaneously, cellular towers near the compound were disrupted to prevent Khamenei's security personnel from issuing warnings during the strike — the camera network and the communications network were both turned against the regime they were built to protect.[17]

---

13 Financial Times. (2026, Mar. 3). Israel hacked Tehran's traffic cameras to track Khamenei ahead of assassination. As reported by Iran International: "Nearly all traffic cameras in Tehran had been hacked for years, with footage encrypted and transmitted to servers in Tel Aviv and southern Israel." https://www.iranintl.com/en/202603027711

14 CNN. (2026, Mar. 3). How the plot to kill Iran's Ayatollah Ali Khamenei came together using hacked traffic cameras in Tehran and U.S. intelligence. IDF Unit 8200 and AI-powered target production described. https://www.cnn.com/2026/03/03/middleeast/us-israel-plot-kill-iran-khamenei-latam-intl. https://www.timesofisrael.com/report-israel-hacked-tehran-traffic-cameras-to-track-khamenei-ahead-of-assassination/

15 Iran International. (2026, Mar. 2). Israel hacked security cameras, phones to track Khamenei. "One camera angle proved particularly useful in determining where bodyguards parked their personal cars and provided insight into the routines inside the compound near Pasteur Street." https://www.iranintl.com/en/202603027711

16 Cybernews. (2026, Mar. 3). Israel hacked Iran's traffic cameras to pinpoint Khamenei. Israeli intelligence official: "We knew Tehran like we know Jerusalem. And when you know [a place] as well as you know the street you grew up on, you notice a single thing that is out of place." https://cybernews.com/editorial/israel-hacked-iran-traffic-cameras-us-war/

17 Jerusalem Post. (2026, Mar. 3). Israel hacked Tehran's traffic cameras, used AI to plan Khamenei's assassination. "Cellular towers in the area had been disrupted so that the security personnel's phones could not receive warning calls." https://www.jpost.com/middle-east/iran-news/article-888598

Iran Tried to Use the Same Tactic Against Israel

The Iran-Israel camera war is bi-directional and it confirms that surveillance infrastructure has become a standard military tool, not an intelligence anomaly.

Since the launch of Operation Roaring Lion on February 28, 2026, Israel's National Cyber Directorate identified over 40

cases in which Iranian groups hacked private and public security cameras for intelligence gathering.[18]

Cybersecurity firm Check Point Research tracked hundreds of Iranian exploitation attempts against Hikvision and Dahua IP cameras across Israel, Qatar, Bahrain, Kuwait, the UAE, Cyprus, and Lebanon, all countries that also experienced missile activity from Iran.[19]

In one documented case during the June 2025 Israel-Iran conflict, Iran compromised a street camera facing Israel's Weizmann Institute of Science and subsequently struck the building with a ballistic missile. The camera was reconnaissance. The missile was the follow-up.[20]

The cameras being exploited by Iran were predominantly Hikvision and Dahua, Chinese-manufactured surveillance products already banned in government buildings in the United States and the United Kingdom for national security vulnerabilities. They remain deployed across Israel, the Gulf states, and critical infrastructure worldwide.[21]

---

18 Ynet News. (2026, Mar. 9). Iran trying to hack hundreds of thousands of Israeli security cameras, cyber directorate says. "Since the launch of Operation Roaring Lion last week, Israel's National Cyber Directorate has identified more than 40 cases in which private or public security cameras were hacked by Iranian groups and other hostile actors for intelligence gathering." https://www.ynetnews.com/tech-and-digital/article/ry0p11rot11x

19 Check Point Research. (2026, Mar. 4). Interplay between Iranian targeting of IP cameras and physical warfare in the Middle East. https://research.checkpoint.com/2026/interplay-between-iranian-targeting-of-ip-cameras-and-physical-warfare-in-the-middle-east/

20 Check Point Research. (2026, Mar. 4). "One of the best-known cases occurred when Iran struck Israel's Weizmann Institute of Science with a ballistic missile and had reportedly taken control of a street camera facing the building just prior to the hit." https://research.checkpoint.com/2026/interplay-between-iranian-targeting-of-ip-cameras-and-physical-warfare-in-the-middle-east/

21 Cybersecurity Dive. (2026, Mar. 4). Iran-nexus hackers target flaws in surveillance cameras. Hikvision and Dahua products targeted via CVE-2017-7921, CVE-2021-33044, CVE-2023-6895, CVE-2025-34067. CISA added CVE-2017-7921 to its Known Exploited Vulnerabilities catalog. https://www.cybersecuritydive.com/news/iran-hackers-target-flaws-ip-cameras/813795/

The Russia Warning—Israeli Software is Already Inside the Kremlin's Cameras

The implications of the Iran operation were not lost on Moscow. And Israel made sure they wouldn't be.

The IDF's Warning to Putin

Following the Khamenei assassination, IDF spokeswoman Anna Ukolova appeared on Russian state radio network RBC and issued an unmistakable warning: Israel controls the webcams in Russia and warns they could target whoever it wants, if Russia moves against Israeli interests. She said Israel has "quite serious capabilities" (citing Iran ops), and if anyone "wishes us evil" they won't be spared—but she hoped "Moscow at this moment does not wish evil to Israel" and "wants to believe it." Implying Russia, and Putin, is vulnerable, just like Iran.[22]

Her exact words: "The elimination of very important people, the top brass, demonstrates Israel's serious capabilities against those who try to wish them harm. I hope that Moscow does not wish harm to Israel at the moment."[23]

This was not bravado. It was a geopolitical signal backed by a technical reality that Russian media scrambled to understand and what they found was alarming.[24]

22 RBC Russia. (2026, Mar. 14). As aggregated by Lemmy.World press review: "Russian media reports IDF spokeswoman Anna Ukolova threatens Russian authorities to be killed if they take anti-Israel position in the war. She said that Israel controls all web-cameras in Russia and could hit easily whoever it wants including Putin." https://lemmy.world/post/44328588, https://www.unz.com/article/idf-threatens-elimination-for-russian-leaders-who-wish-israel-ill/. https://scheerpost.com/2026/03/19/idf-threatens-elimination-for-russian-leaders-who-wish-israel-ill/

23 Pravda EN. (2026, Mar. 16). "I hope Moscow does not want to harm Israel": is the IDF threatening "very important people" in Russia? Full Ukolova quote reproduced. https://news-pravda.com/world/2026/03/16/2158496.html

24 Hvylya. (2026, Mar. 13). Israeli Software BriefCam Found in Russian Surveillance Systems Following Khamenei Assassination. https://en.hvylya.net/news/1296-israeli-software-briefcam-found-in-russian-surveillance-systems-following-khamenei-assassination

BriefCam: Israeli Software Embedded in Russian Surveillance Systems

Russian investigative outlet The Moscow Times and Telegram channel Mash reported that BriefCam, the Israeli-developed AI video analytics software used to hack cameras in Tehran, was found embedded in Russian video surveillance networks.[25]

25 The Moscow Times / Mash Telegram channel. (2026, Mar.). As reported by Hvylya (2026, Mar. 13): "Israeli reconnaissance software BriefCam, with which cameras were hacked in Tehran, were found in Russian surveillance cameras." https://en.hvylya.net/news/1296-israeli-software-briefcam-found-in-russian-surveillance-systems-following-khamenei-assassination

BriefCam is a deep video stream analysis platform capable of recognizing human actions, vehicle movements, and behavioral patterns. It processes massive datasets, searching archives for specific events and generating intelligence summaries.[26]

BriefCam was acquired by Canon in 2018 and subsequently integrated into VMS XProtect, a video management system developed by Danish company Milestone Systems. Milestone officially exited Russia in 2022 following sanctions. The software, however, never left. Market experts reported it continues to operate through gray-market imports and cracked installations.[27]

State contracts in Russia indicate that suppliers of VMS XProtect won multiple government tenders—meaning Israeli-origin surveillance software may be embedded in Russian government infrastructure.[28]

The irony is staggering and the lesson is stark: the surveillance architecture a state deploys to control its population can become the very weapon used to destroy its leadership.

26 Hvylya. (2026, Mar. 13). "BriefCam is designed for deep video stream analysis, capable of recognizing specific human actions and vehicle movements. The platform automatically processes massive datasets, searching archives for specific events and generating visual summaries." https://en.hvylya.net/news/1296-israeli-software-briefcam-found-in-russian-surveillance-systems-following-khamenei-assassination

27 Hvylya. (2026, Mar. 13). "BriefCam's developer was acquired by the Japanese corporation Canon in 2018. The technology was later integrated into the VMS XProtect system by the Danish company Milestone Systems. While Milestone Systems officially exited the Russian market in 2022, the use of XProtect and BriefCam continues. Market experts suggest that some distributors offer these products through gray import schemes or install cracked versions of the software." https://en.hvylya.net/news/1296-israeli-software-briefcam-found-in-russian-surveillance-systems-following-khamenei-assassination

28 Lemmy.World press review citing Mash Telegram channel. (2026, Mar. 14). "Suppliers of VMS XProtect, according to the telegram channel, won several state tenders in Russia." https://lemmy.world/post/44328588

Chinese Camera Brands are Compromised by Design

Hikvision and Dahua, the two largest surveillance camera manufacturers in the world, supplying products to over 200 countries, have been banned from U.S. government use, placed on the FCC's Covered List as national security threats, and restricted or removed in the UK, Australia, and multiple European nations.[32]

32 IPVM Public Report. (2024). Where Dahua and Hikvision Are Banned. https://ipvm.com/reports/hikua-bans. FCC (2021): Hikvision and Dahua designated as national security threats, placed on Covered List banning new imports or sales in the USA. See also: Oxford Academic / Journal of Cybersecurity. (2025). Cyber vulnerabilities and technical regulation of China-made CCTV IoT surveillance cameras in Australia. https://academic.oup.com/cybersecurity/article/11/1/tyaf039/8345066

China's Surveillance Export—Sowing the Seeds of Its Own Destruction

No actor in the global surveillance economy has more to lose from the Iran precedent than the Chinese Communist Party. Beijing has spent the last decade building, deploying, and exporting the most sophisticated mass surveillance apparatus in human history. It has sold that apparatus to dozens of authoritarian allies as a "stability maintenance" solution. Iran was among its most eager customers.

China Supplied Iran's Surveillance State

Iran's surveillance infrastructure, the very camera network Israel hacked, was built largely on Chinese technology, including smart cameras, facial recognition systems, and internet-filtering equipment supplied through a decade-long security partnership between Tehran and Beijing.[29]

This same infrastructure was used to suppress the Iranian protests that erupted in late 2025, enabling near-total internet shutdowns, mobile network disruptions, and mass identification of protesters, leading to a death toll that independent human rights organizations estimated in the thousands.[30]

The systems that crushed internal dissent were the same systems that were subsequently turned against the regime's own leaders by a foreign adversary. China's export model built a trap and its client walked into it.[31]

---

29 Probe International Journal. (2026, Mar. 12). Protests exposed regime's reliance on Chinese surveillance tech. "These include 'smart' cameras, facial recognition for identifying and tracking protesters, internet-filtering equipment, and elements including the BeiDou GPS system. This support stems from a decade-long security partnership between Iran and China." https://journal.probeinternational.org/2026/03/12/protests-exposed-regimes-reliance-on-chinese-surveillance-tech/

30 Probe International Journal. (2026, Mar. 12). Reports from Article 19 cited: "These technologies facilitated near-total nationwide internet shutdowns (starting around January 8, 2026), mobile network disruptions, and censorship, isolating Iran's ~93 million citizens from the global internet." Death toll estimated at 5,000-36,500 by independent human rights organizations. https://journal.probeinternational.org/2026/03/12/protests-exposed-regimes-reliance-on-chinese-surveillance-tech/

31 Probe International Journal. (2026, Mar. 12). "For Beijing, which has aggressively marketed its 'stability maintenance' model to allied autocracies while deploying the world's most extensive domestic surveillance apparatus to quash internal dissent, this serves as a cautionary tale: the same systems empowering control over populations could one day be turned inward or against the Chinese Communist Party itself." https://journal.probeinternational.org/2026/03/12/protests-exposed-regimes-reliance-on-chinese-surveillance-tech/

Both companies are deeply intertwined with the CCP. China's Military-Civil Fusion policy requires that private firms share technology and data with the People's Liberation Army. Hikvision and Dahua are not exceptions, they are prime examples.[33]

The vulnerabilities being exploited by Iranian hackers to surveil Israel and Gulf states, CVE-2017-7921, CVE-2021-33044, CVE-2023-6895, are known, patched flaws that remain unaddressed on millions of deployed devices globally, including in critical infrastructure.[34]

Ukraine provides the precedent for what is at stake: Russian intelligence hacked Chinese-made Hikvision cameras in Kyiv to observe infrastructure targets and air defense positions. When Russian missiles struck Kyiv on January 2, 2024, the SBU confirmed that compromised CCTV cameras, including a parking lot camera and a condominium camera, helped guide the strike.[35]

For the CCP, the strategic lesson is this: the surveillance infrastructure it has deployed domestically and exported globally is not secure. Any adversary that can penetrate it, as Israel penetrated Iran's, gains not just intelligence but a kill chain. **The very cameras that empower authoritarian control are also the cameras that can be turned against the Party itself.**[36]

---

33 White House. (2019). Executive Order on ICT Supply Chains. China's Military-Civil Fusion policy requires private sector firms to cooperate with the PLA. As cited in Walker, R. Chinese Land Ownership, EMP Threats, and Surveillance in the United States: National Security Implications (2025). https://www.securitysales.com/news/dahua-chinese-military-dod-blacklist/146782/. https://www.securityinfowatch.com/video-surveillance/article/21144071/defense-department-names-hikvision-on-list-of-companies-linked-to-chinese-military

34 Cybersecurity Dive. (2026, Mar. 4). Iran-nexus hackers target flaws in surveillance cameras. CVEs exploited: CVE-2017-7921, CVE-2021-33044, CVE-2023-6895, CVE-2025-34067. CISA KEV catalog addition confirmed. https://www.cybersecuritydive.com/news/iran-hackers-target-flaws-ip-cameras/813795/

35 RFE/RL Schemes Investigation. (2024, Feb. 15). China's Hikvision, Dahua Security Cameras Heighten Risks of Russian Attacks on Ukraine. "When Russian missiles struck Kyiv in a January 2 attack that killed at least three people, two ordinary outdoor CCTV cameras helped guide their way, the State Security Service of Ukraine (SBU) claims." https://www.rferl.org/a/ukraine-cameras-china-security-risks-hikvision-dahua-schemes-investigation/32810571.html

36 Probe International Journal. (2026, Mar. 12). Protests exposed regime's reliance on Chinese surveillance tech. The Iran case as a cautionary tale for CCP's own surveillance infrastructure. https://journal.probeinternational.org/2026/03/12/protests-exposed-regimes-reliance-on-chinese-surveillance-tech/

The American Home—A Surveillance Outpost in Every Neighborhood

The threats described above are not confined to foreign battlefields or authoritarian regimes. The same architecture, insecure, networked, AI-powered, and increasingly corporate-law enforcement integrated, is being built inside American homes, one Ring doorbell and DJI robot vacuum at a time.

As of 2020, 54 million U.S. households had at least one smart home device installed. Market research indicates that those who already own one typically want more. The surveillance footprint inside American homes is expanding, not contracting.[37]

Ring cameras, Google Nest doorbells, and smart home assistants such as Amazon Alexa and Google Home are always-on listening

37 Parks Associates. (2020). Approximately 54 million U.S. households had at least one smart home device installed as of 2020. As cited in Popular Science. (2026, Feb. 21). Man accidentally gains control of 7,000 robot vacuums. https://www.popsci.com/technology/robot-vacuum-army/

and recording devices. In a documented case, Google was able to retrieve footage from a Nest doorbell camera to assist in an abduction investigation, despite earlier indications that the footage had been permanently deleted. The footage was not deleted. Raising the question, is it ever deleted?[38]

Router vulnerabilities compound the risk. Brands including Huawei, TP-Link, and ZTE have been documented to contain exploitable firmware backdoors that allow hackers to monitor internet activity, breach connected security systems, and disable alarm functions silently, remotely, and in real time.[39]

DJI drones, widely used by law enforcement, real estate professionals, and hobbyists, have been documented to transmit user data, GPS coordinates, and flight logs to servers in China. The Department of Defense has listed DJI on its Chinese Military Industrial Complex list.[40]

The next generation of home surveillance is already being marketed: humanoid robots from companies like Tesla, Figure, and 1X that live in your home, perform domestic tasks, and require unprecedented access to the intimate details of your household environment to function. For a stalker, a corporate data harvester, or a foreign intelligence service, that represents a targeting goldmine.[41]

---

38 The Verge. (2026, Feb.). Google was able to retrieve footage from a Nest Doorbell camera to assist in an abduction investigation despite earlier indications that footage had been deleted. As cited in Popular Science. (2026, Feb. 21). https://www.popsci.com/technology/robot-vacuum-army/. https://arstechnica.com/google/2026/02/google-recovers-deleted-nest-video-in-high-profile-abduction-case/

39 Goodin, D. (2021). Security Flaws Found in Popular Home Routers. Ars Technica. Huawei, TP-Link, ZTE documented firmware backdoors. As cited in Walker, R. Protecting Individual Privacy and Securing the Nation from 5th Generation Foreign Threats (2025). https://arstechnica.com/tech-policy/2024/12/report-us-considers-banning-tp-link-routers-over-security-flaws-ties-to-china/#:~:text=In%20May%202023%2C%20Check%20Point,by%20Chinese%20state%2Dsponsored%20attackers. https://arstechnica.com/tech-policy/2024/12/report-us-considers-banning-tp-link-routers-over-security-flaws-ties-to-china/#:~:text=In%20May%202023%2C%20Check%20Point,by%20Chinese%20state%2D-sponsored%20attackers.

40 U.S. Department of Defense. (2021). CMIC Listings. DJI drones documented to transmit user data, GPS coordinates, and flight logs to servers in China. As cited in Walker, R. Protecting Individual Privacy and Securing the Nation from 5th Generation Foreign Threats (2025). https://www.scmp.com/news/us/article/3327057/drone-maker-dji-loses-lawsuit-against-pentagon-claim-chinese-military-ties

41 Popular Science. (2026, Feb. 21). Man accidentally gains control of 7,000 robot vacuums. "Eventually, for any of these at-home robot servants to function effectively, they will need unprecedented access to the intimate details of their owners' homes. For a stalker or hacker, that represents a potential goldmine." https://www.popsci.com/technology/robot-vacuum-army/

What Must Be Done—A Call to Action

We are not helpless. But inaction is no longer an option. The Iran operation has proven, publicly, irrefutably, and with lethal consequence, that surveillance cameras are weapons. The question for American policymakers, consumers, and national security professionals is simple: are we building our own telescreen, or are we going to dismantle it before someone else turns it against us?

The Rainey Center's March 2026 national poll of 1,021 registered voters confirms that the American public is ready for action. **63%** are concerned that security cameras in American homes and government buildings may use Chinese-made software allowing foreign access to footage. **72%** are concerned that this data is being used by foreign governments to develop competing AI. And when asked about specific policy responses, the numbers are overwhelming: **68%** support state legislation banning personal data storage in Chinese data centers and requiring hardware and software certification—the strongest policy number in the entire survey. **51%** support banning Chinese-developed software in U.S. security cameras. The political ground for every recommendation that follows is not speculative—it is empirical.

Implement a national Privacy Gold Star Certification, a mandatory labeling and compliance system that distinguishes trustworthy IoT devices from surveillance vectors, requiring U.S.-only software and firmware, U.S.-based data storage, end-to-end encryption, and explicit opt-in consent for all data collection.[42]

Permanently ban Hikvision, Dahua, DJI, TP-Link, Huawei, and ZTE products from all U.S. critical infrastructure, government facilities, schools, and law enforcement use and personal use in the borders of the United States. The FCC ban on new imports is a start. It is not sufficient.[43]

Mandate that all law enforcement access to civilian camera footage require a judicial warrant. The Ring-Flock arrangement that allowed ICE warrantless access to neighborhood camera networks through a side-door corporate partnership is precisely the kind of Fourth Amendment erosion that must be legislatively closed.[44]

Require affirmative opt-in for AI-powered features on all networked home devices. The default setting should always protect privacy, not aggregate data for corporate or law enforcement benefit.[45]

Launch a national public awareness campaign that treats unsecured home surveillance devices as a security risk equivalent to an unlocked front door, because in the age of AI-

---

42 Walker, R. Protecting Individual Privacy and Securing the Nation from 5th Generation Foreign Threats (2025). Privacy Gold Star Certification framework proposed. See also: Westin, A. (2019). Privacy and Freedom. Atheneum.

43 FCC Covered List (2021). Huawei, ZTE, Hytera, Hikvision, Dahua banned from new equipment authorization in the United States as national security threats. See also: Cyber Magazine. (2026, Jan. 19). Inside China's ban of major U.S. and Israeli cyber firms. https://cybermagazine.com/news/inside-chinas-ban-of-major-us-and-israeli-cyber-firms

44 404 Media / Yahoo News. (2026, Feb. 13). Local police departments searching Flock's camera network on behalf of ICE and CBP through a side-door access arrangement without formal contracts. Ring's Community Requests feature allows law enforcement to access footage without warrants in some circumstances. https://www.yahoo.com/news/us/article/why-that-ring-super-bowl-ad-about-finding-your-lost-dog-is-creeping-people-out-211647194.html

45 Truthout. (2026, Feb. 9). Super Bowl Ad for Ring Cameras Touted AI Surveillance Network. "Guariglia noted that Ring would likely make the AI-powered features on by default, requiring users to manually search their settings to turn it off." https://truthout.org/articles/super-bowl-ad-for-ring-cameras-touted-ai-surveillance-network/

powered camera hacking, that is precisely what they are.[46]

Ban the storage of American citizens' data in Chinese-controlled data centers. Any device, application, platform, or cloud service operating in the United States must store and process U.S. user data exclusively on servers physically located within the United States and operated by entities free of foreign adversary ownership or influence. The pipeline that flows from an American's home camera to a server in Shenzhen is not a business arrangement, it is a national security threat. Congress must close it by statute, with criminal penalties for violations, not voluntary compliance frameworks that bad actors ignore.[47]

Prohibit Chinese-developed software from being embedded in hardware sold or deployed in the United States. This is not merely a consumer protection measure, it is a battlefield imperative. The BriefCam precedent proved that software developed by an adversary nation can be quietly embedded in surveillance infrastructure and later weaponized for targeting and intelligence collection. Under China's Military-Civil Fusion doctrine, any software produced by a Chinese firm is potentially dual-use by legal mandate. No Chinese-origin firmware, operating system, analytics engine, or AI model should be permitted inside cameras, routers, drones, IoT devices, or any networked hardware operating on American soil. Hardware certification must include full software provenance auditing, with independent verification that no component of the software stack originates from a foreign adversary nation.[48]

---

46 Ynet News. (2026, Mar. 9). Iran trying to hack hundreds of thousands of Israeli security cameras. "For even a novice hacker, locating an unsecured camera can take only minutes. Websites such as Shodan scan the internet and map connected devices worldwide." https://www.ynetnews.com/tech-and-digital/article/ry0p11rot11x

47 Walker, R. Chinese Land Ownership, EMP Threats, and Surveillance in the United States: National Security Implications (2025). DJI documented to transmit data to Chinese servers; Hikvision and Dahua cloud platforms subject to CCP data access laws under China's National Intelligence Law (2017), which requires all Chinese organizations to support, assist, and cooperate with Chinese state intelligence work. https://www.scmp.com/news/us/article/3327057/drone-maker-dji-loses-lawsuit-against-pentagon-claim-chinese-military-ties

48 Hvylya. (2026, Mar. 13). Israeli Software BriefCam Found in Russian Surveillance Systems. BriefCam precedent: adversary-origin software embedded in surveillance infrastructure weaponized for targeting. https://en.hvylya.net/news/1296-israeli-software-briefcam-found-in-russian-surveillance-systems-following-khamenei-assassination. See also: White House. (2019). Executive Order on ICT Supply Chains re: Military-Civil Fusion dual-use mandate.

CONCLUSION

The Telescreen is Already On

George Orwell's telescreen watched you whether you wanted it to or not. The Party told you it was for your protection. It told you it would keep you safe, keep your neighborhood safe, help you find your lost dog.

We have built that telescreen ourselves. We have installed it at our front doors, mounted it in our hallways, rolled it across our floors, and attached it to the underside of drones we fly over our own neighborhoods. We have handed the footage to corporations, who have handed it to law enforcement, who have

handed it to federal agencies without warrants, oversight, or accountability.

And now we know, because Israel proved it in real time, on a real target, with a real missile, that those cameras are not just watching. They are targeting.

The Iranian regime built one of the most sophisticated surveillance states in the Middle East with Chinese technology and CCP expertise. It used those cameras to hunt protesters, silence dissidents, and enforce compliance. Then Israel hacked those same cameras, mapped the movements of the Supreme Leader's bodyguards, and ended his life.

For Beijing, watching all of this unfold, the message should be existential. The surveillance empire the CCP has built, domestically and globally, is not a fortress. It is a vulnerability. The same systems built to ensure the Party's permanent control could one day be the instrument of its unraveling.

For American citizens, the message is more immediate. The cameras watching your street, your front door, and your living room floor are not neutral. They have owners, they have vulnerabilities, and they have the attention of foreign intelligence services, domestic law enforcement, and corporate data brokers who see your home as an asset to be mined.

Orwell's Winston Smith famously wrote in his diary: *"Big Brother is watching you."*

He had no idea how right he was—or how willing we would be to let it happen.

Russ Walker is a policy and campaign advisor with almost three decades of experiences advising policy makers and policy organizations. Today he serves as the VP of Policy for The Joseph Rainey Center for Public Policy and the Executive Director of the Rainey Freedom Project.

Rainey
Center

info@raineycenter.org
raineycenter.org