UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

DIANA KOVALENKO (alias), TARAS KOVALENKO (alias); LIUBOV SAVCHENKO, individually and as next friend of V.S., a minor; VASYL SHESTAK; VALERII KOBYLIANSKYI; OLENA KOBYLIANSKA; and SVITLANA TSYLINKO, individually and as next friend of D.T., a minor;

Plaintiffs,

- against -

UBIQUITI, INC.,

Defendant.

Case No. _____

JURY TRIAL DEMANDED

CAUSES OF ACTION

1) Negligent Entrustment
2) Public Nuisance
3) Strict Products Liability – Design Defect
4) Negligent Product Design
5) Negligent Infliction of Emotional Distress
6) Aiding and Abetting Assault
7) Aiding and Abetting Battery
8) Aiding and Abetting Intentional Infliction of Emotional Distress

COMPLAINT

"*It can't happen again. If it does, I'll be in a lot of trouble*."

– Ubiquiti CEO Robert Pera, on Ubiquiti's violation of U.S. sanctions.[1]

[1] Kerry A. Dolan, *Silicon Valley's Newest Billionaire: Wireless Wonder Robert Pera*, Forbes (Jan. 3, 2012), https://www.forbes.com/forbes/2012/0116/entrepreneurs-robert-pera-computer-hardware-apple.html.

TABLE OF CONTENTS

Upon personal knowledge and/or information and belief, Plaintiffs Diana Kovalenko (alias); Taras Kovalenko (alias); Liubov Savchenko, individually and as next friend of V.S., her minor child; Vasyl Shestak; Valerii Kobylianskyi; Olena Kobylianska; and Svitlana Tsylinko, individually and as next friend of D.T., her minor child, (collectively, "Plaintiffs") allege against Defendant Ubiquiti, Inc., as follows.

INTRODUCTION

1. The Russian drones come from above. A buzzing sound cuts the blue sky of Ukraine. A boy on a bicycle. A mother and child at a market. A camera is training digital crosshairs on them.

2. The drone operators call themselves the "hunters." In invaded Ukraine, they have imposed a "kill zone" where drones hunt civilians in a "human safari"—a campaign of high-tech murder condemned by the United States and international community as crimes against humanity.

3. The Russian hunters coordinate the safari using military communications technology designed and distributed by a New York-based company—Defendant Ubiquiti, Inc.—in violation of U.S. export controls and international arms-control mechanisms.

4. Ubiquiti produces encrypted radio bridge antennas, a battlefield communications system that networks devices up to 100 km apart. Russia uses Ubiquiti radio bridges to link reconnaissance, drone operators, artillery, and commanders in a military command-and-control system instrumental to the occupation of Ukraine.

5. After the 2022 invasion, the United States banned all exports of these devices to Russia. The federal government warned Ubiquiti that its devices are dangerous instrumentalities

that Russia "needs to sustain its brutal attack on Ukraine" and are "used in Russian weapons systems."[2]

6. Ubiquiti kept selling anyway—through a chain of distributors in Eastern Europe and Central Asia that bore every hallmark of sanctions evasion. After the initial Russian invasion in 2014, Ubiquiti CEO Robert Pera publicly admitted "we know that there's a couple other guys that more than likely move some products into Russia."

7. Rather than cut off these Russian distributors and vendors, Ubiquiti quietly scrubbed them from its website. But out of public view, Ubiquiti kept supplying banned devices to them in a process that armed the Russian military through Russian-language websites using Ubiquiti's own brand, including www.ubiquiti.ru.

8. Under the export ban, Ubiquiti exports to Russia should have been zero. Instead, they surged by over 60% after the 2022 invasion. From March to October 2022, Ubiquiti directly shipped banned military-communications gear to its Russian distributors, who armed the invading forces. Then, it shifted to supplying Russia's military through notorious smuggling hubs in Turkey, Czechia, and Kazakhstan. U.S. authorities warned Ubiquiti that these were high-risk, red-flag jurisdictions for sanctions evasion. But that did not stop Ubiquiti from shipping more than an estimated 100,000 banned devices that the U.S. government deemed "necessary to fuel Russia's war machine."[3]

9. Ubiquiti knows that it is arming Russia's occupation or is willfully blind to this fact.

---

[2] Bureau of Indus. & Sec., U.S. Dep't of Com., *Common High Priority Items List (CHPL)* (Feb. 23, 2024), https://www.bis.gov/licensing/country-guidance/common-high-priority-items-list-chpl [hereinafter Bureau of Indus. & Sec., U.S. Dep't of Com., *High Priority Items List*].

[3] *Id.*

10. U.S. law requires Ubiquiti to monitor its distribution chain, verify its end-users, and refrain from arming Russia. And with 1,600 employees and some $2.6 billion in revenue in 2025, Ubiquiti has all the resources needed to run an effective compliance program in New York.

11. Ubiquiti admitted to investors and the SEC that it is "monitoring" the conflict in Ukraine. Over the past four years, its monitors would have seen Russian state television and social media repeatedly broadcast videos of Russian soldiers installing Ubiquiti antennas in occupied Ukraine. On state television, the Russian Ministry of Defense praised Ubiquiti devices as indispensable to "the effectiveness of unit command and control" in the "special military operation"—Russia's euphemism for the occupation of Ukraine.

12. Over the years, tens of thousands of banned devices "phoned home" to Ubiquiti's servers to receive software updates. Defendant's own telemetry data told it these banned devices were operating in Russia and occupied Ukraine.

13. Ubiquiti could have stopped this. It had the contractual power to terminate any distributor who evaded U.S. sanctions. It could have written a kill switch and a whitelist into firmware updates that it supplied to Russian occupation forces—the same life-saving design feature SpaceX took in February 2026, when it geofenced and deactivated Starlink terminals that Russian forces were installing in drones for navigation. Ubiquiti did none of these things.

14. Ubiquiti refused to cut off Russia's command-and-control infrastructure even after a January 2026 investigative report by Hunterbrook Media exposed the smuggling scheme in detail. It still refused after the world-famous Russian dissident band Pussy Riot staged a protest at Ubiquiti's Manhattan headquarters in March 2026. Six months later, Ubiquiti still has not cut off a prominent Czech distributor caught arming the Russian military-procurement pipeline and it continues to supply the Russian occupation through its distribution network.

15. In short, Ubiquiti supplied—and continues to supply—large volumes of banned military-communications devices to Russia in violation of federal law, it took steps to conceal that unlawful distribution, and it did all this against a backdrop of repeated warnings by U.S. authorities.

16. The results were foreseeable. Russian forces continue to deploy Ubiquiti devices to occupy Ukraine and track down and kill civilians. And despite Ukrainian forces' effort to search and destroy the antennas, Russia replaces them from a seemingly inexhaustible supply.

17. In occupied Ukraine and along the Russian border, the Russian military is using the command-and-control system powered by Ubiquiti to wage the human safari. They hunt by videoconference—commanders and drone operators watch streamed footage from reconnaissance drones and decide who should die.

18. Plaintiffs are Ukrainian victims of the human safari. On September 2, 2024, Doctors Max and Diana Kovalenko were driving through their neighborhood in Kherson when a Russian drone chased their car and dropped a bomb through the windshield. Max was killed. Diana was maimed. The drone unit shared a trophy video online, praising the "hunter's" precision. When their son Taras later visited his father's grave, a Russian drone hunted him too.

19. On August 12, 2025, the safari came for husband and wife Valerii and Olena Koblylianskyi in Chernihiv Province. A Russian drone stalked the parking lot of the power plant where they worked, exploding into Valerii in front of Olena's eyes and leaving shrapnel embedded in his pelvis.

20. On September 13, 2025, it came for Vasyl Shestak, a firefighter in the border village of Kostobobriv. He answered a call from a friend under drone attack. A Russian drone hunted him

down and detonated near him, tearing through his ribs and organs. He survived but can no longer work as a first responder.

21. On October 10, 2025, it came for Anatoliy Savchenko when a Russian drone attacked his car and, minutes later, another attacked his rescuers, killing him in a double-tap strike. Like other civilians in the kill zone, his widow, Liubov, and son, S., live in fear of the hunt.

22. On May 27, 2026, it came for Svitlana Tsylinko and her seven-year-old son D., who were severely injured after a Russian drone struck the courtyard of their apartment in Kherson City.

23. They are not alone. Hundreds of civilians have been killed, and thousands wounded or forcibly displaced, by the human safari coordinated through banned Ubiquiti devices that Defendant supplied and serviced in violation of U.S. export controls.

24. Plaintiffs seek to hold Ubiquiti liable under New York law for negligently entrusting these banned devices to Russia—even though it knew or should have known of the dangers of equipping Russian occupation forces. They also bring claims for defective product design, public nuisance, negligent infliction of emotional distress, and aiding and abetting assault, battery, and intentional infliction of emotional distress.

JURISDICTION AND VENUE

25. There is subject matter jurisdiction under 28 U.S.C. § 1332(a)(2) because Plaintiffs are citizens of Ukraine and Ubiquiti is a citizen of New York.

26. This Court has general personal jurisdiction over Ubiquiti because Ubiquiti is at home in New York, where it maintains its principal place of business.

27. Venue is proper under 28 U.S.C. § 1391(b)(1) and (b)(3). Ubiquiti resides in this District, and its alleged acts and omissions occurred in this District. Ubiquiti maintained its

headquarters, entered into and administered its distribution agreements, exercised compliance oversight over its distribution channel, and designed and approved the airMAX firmware, all from this District.

PARTIES

Plaintiffs

28. **Valerii Kobylianskyi** is a citizen and resident of Ukraine. On or about August 12, 2025, he was gravely injured by a Russian drone attack in the parking lot of the civilian power station where he worked in Semenivka, Chernihiv Province, less than 20 km from the Russian border, within the kill zone.

29. **Olena Kobylianska** is a citizen and resident of Ukraine and the spouse of Plaintiff Valerii Kobylianskyi. She was working at the same civilian power station as her husband during the drone attack on or about August 12, 2025. She suffered severe emotional distress by surviving the attack and personally observing her husband being injured in the explosion.

30. **Diana Kovalenko** (alias) is a citizen and resident of Ukraine. She is the widow of Max Kovalenko (alias), killed in a Russian drone attack in Kherson on or about September 2, 2024. She was maimed in the same attack and was displaced from her home. She proceeds under a pseudonym for fear of retaliation by the Russian regime. She resided with Max at the time of his death and is a legal heir, by intestate succession, with a vested right to recover economic and non-economic damages under Ukrainian law.

31. **Taras Kovalenko** (alias) is a citizen and resident of Ukraine and the adult son of Max and Diana Kovalenko. He suffered emotional harm from his father's murder, from being chased by a Russian drone at his father's grave, and from his displacement from Kherson. He proceeds under a pseudonym for fear of retaliation.

32. **Liubov Savchenko** is a citizen and resident of Ukraine. She is the surviving widow of Anatoliy Savchenko, killed in a Russian drone attack in Chernihiv Province on or about October 10, 2025. She also brings claims as parent and legal guardian of V.S., Anatoliy's surviving minor son (age 17). Liubov and V.S. resided with Anatoliy at the time of his death and are legal heirs, by intestate succession, with a vested right to recover economic and non-economic damages under Ukrainian law.

33. **Vasyl Shestak** is a citizen and resident of Ukraine, where he serves as a firefighter. On or about September 13, 2025, he was gravely injured by a Russian drone while responding to a friend's call for help in Kostobobriv, Chernihiv Province.

34. **Svitlana Tsylinko** is a citizen and resident of Ukraine displaced by the conflict. She also brings claims as parent and legal guardian of D.T., her minor son (age 7). On May 27, 2026, Svitlana and D.T. were severely injured after a Russian drone struck the courtyard of Svitlana's apartment in Kherson.

Defendant

35. Ubiquiti Inc. is a Delaware corporation with its principal place of business at 685 Third Avenue, New York, New York 10017.

36. Ubiquiti designs, manufactures, and markets military-grade wireless communications hardware and software—including the airMAX radio bridge product line at issue here—that is restricted under U.S. export controls and arms control treaties.

37. Ubiquiti's founder and CEO, Robert Pera, directs Ubiquiti's operations from New York.

FACTUAL ALLEGATIONS

I. Russia launches a "brutal attack on Ukraine," subjecting civilians to crimes against humanity.

38. Russia first invaded Ukraine in 2014, forcibly annexing Crimea and seizing parts of eastern Ukraine. Then, on February 24, 2022, Russia launched a full-scale invasion and occupation—the largest war of territorial aggression in Europe since World War II.

39. From the outset, Russia carried out a campaign of atrocities targeting civilians. The United States launched war crimes investigations and, on March 23, 2022, the U.S. State Department announced that "the U.S. government assesses that members of Russia's forces have committed war crimes in Ukraine" citing evidence of "attacks deliberately targeting civilians" including strikes on sites "clearly identifiable as in-use by civilians" including "schools, hospitals, . . . civilian vehicles, shopping centers, and ambulances."[4] On February 18, 2023, the U.S. Secretary of State made the formal determination that "members of Russia's forces and other Russian officials have committed crimes against humanity in Ukraine."[5] The U.S. government determined that "[t]hese acts are not random or spontaneous; they are part of the Kremlin's widespread and systematic attack against Ukraine's civilian population."

40. The atrocities were openly exposed and documented in reports by the U.S. government, United Nations, NGOs, and media. Throughout Ukraine, Russian forces have targeted civilians with bombing, artillery, and drone strikes. Russian ground units have conducted "cleansing" operations, abducting, torturing, raping, and summarily executing Ukrainian civilians.

[4] "War Crimes by Russia's Forces in Ukraine," Press Statement, Sec'y of State Anthony J. Blinken, Mar. 24, 2022, https://id.usembassy.gov/war-crimes-by-russias-forces-in-ukraine/

[5] "Crimes Against Humanity in Ukraine", Press Statement, Sec'y of State Anthony J. Blinken, Feb. 18, 2023, https://2021-2025.state.gov/crimes-against-humanity-in-ukraine/.

Thousands of Ukrainian children have been forcibly separated from their parents and transferred to Russian adults for indoctrination or military conscription.

41. In September 2022, Russia formally annexed the Ukrainian Provinces of Kherson, Zaporizhzhia, Donetsk, and Luhansk, despite Ukrainian counter-offensives. To this day, it continues to attack and seize territory across Chernihiv, Sumy, Kharkiv, Dnipropetrovsk, and Mykolaiv Provinces, while launching longer range strikes into the capital, Kyiv, and other regions further from the front lines.

42. As of late 2025, Russian attacks have killed or injured over 50,000 Ukrainian civilians and displaced over 10 million Ukrainians from their homes.

II. The U.S. imposes sanctions, banning the export of Ubiquiti military communications technology to Russia.

43. In response to Russia's invasion, the United States imposed sanctions and "stringent export controls that restrict Russia's access to the technologies and other items that it needs to sustain its brutal attack on Ukraine."[6]

44. Even before the Russia sanctions, Ubiquiti's military communications equipment was already strictly regulated under U.S. export control law and the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies—an international arms control agreement.[7]

45. Under this treaty and U.S. implementing statutes, Ubiquiti's airMax radio bridges—long-range antennas that create encrypted communication networks in battlefields and

[6] Bureau of Indus. & Sec., U.S. Dep't of Com., *High Priority Items*, *supra* note 2; U.S. Gov't Accountability Off., GAO-25-107079, *Russia Sanctions and Export Controls: U.S. Agencies Should Establish Targets to Better Assess Effectiveness* (2025), https://www.gao.gov/assets/gao-25-107079.pdf.

[7] *See* Bureau of Industry and Security, *Encryption Controls*, https://www.bis.gov/learn-support/encryption-controls (explaining that the 5A002 designation on the U.S. Commerce Control List implements the Wassenaar Arrangement controls on dual-use encryption technologies).

remote areas—are subject to the highly restrictive Export Control Classification Number 5A002 and licensing requirements.[8]

46. Beginning in 2014, the United States layered Russia-specific restrictions on top of that baseline: sectoral sanctions on Russia's defense sector under Executive Order 13662; and, in December 2014, a comprehensive embargo on Russian-annexed Crimea under Executive Order 13685.

47. In 2020, the Commerce Department's Bureau of Industry and Security ("BIS") extended its Military End-Use and End-User Rule to Russia, 15 C.F.R. § 744.21, requiring a license—presumptively denied—for any 5A002 item destined for a Russian military end user or end use. In December 2021, BIS added a parallel rule for Russian military-intelligence end users, 15 C.F.R. § 744.22.

48. Then on February 24, 2022, hours after the full-scale invasion, BIS effectively banned the export, reexport, or in-country transfer of any Commerce Control List item—including Ubiquiti's 5A002 devices—to or through Russia. 15 C.F.R. § 746.8(a)(1), (b).[9] On March 2, 2022, BIS extended the same regime to Belarus and closed the "ENC" License Exception that had previously permitted the sale of 5A002 devices to non-governmental end users for civilian use in Russia.[10]

---

[8] Ubiquiti Networks, Inc., *US Export Controls on Ubiquiti Products* 2 (Nov. 19, 2015), https://dl.ubnt.com/ubnt_export_control_info.pdf.

[9] U.S. Dep't of Com., Bureau of Indus. & Sec., Press Release, *Commerce Implements Sweeping Restrictions on Exports to Russia in Response to Further Invasion of Ukraine* (Feb. 24, 2022), https://www.bis.gov/press-release/commerce-implements-sweeping-restrictions-exports-russia-response-further-invasion-ukraine [hereinafter U.S. Dep't of Com., Bureau of Indus. & Sec., *Sweeping Restrictions*]. The final rule was published on March 3, 2022, but made effective February 24, 2022. *Implementation of Sanctions Against Russia Under the Export Administration Regulations (EAR)*, 87 Fed. Reg. 12,226, 12,226 (Mar. 3, 2022), https://www.govinfo.gov/content/pkg/FR-2022-03-03/pdf/2022-04300.pdf.

[10] U.S. Dep't of Com., Bureau of Indus. & Sec., Press Release, *Commerce Imposes Sweeping Export Restrictions on Belarus for Enabling Russia's Further Invasion of Ukraine* (Mar. 2, 2022), https://www.bis.gov/press-release/commerce-imposes-sweeping-export-restrictions-belarus-enabling-russias-further-invasion-ukraine; *Imposition of Sanctions Against Belarus Under the Export Administration Regulations (EAR)*, 87 Fed. Reg.

49. As of March 2, 2022, Ubiquiti's airMax devices were thus banned from reaching Russia—without exception—unless specifically authorized by BIS. AirMAX software updates and other kinds of technical support were also restricted.

50. As Russia's occupation progressed, the United States ramped up enforcement, singling out military-communications equipment. On January 23, 2024, BIS added antennas to Supplement No. 7 of Part 746, determining they played an "indispensable role" in Russian drones and military field communications.[11]

51. On February 23, 2024, BIS published its Common High Priority Items List—items that the U.S. government has designated as "necessary to fuel Russia's war machine."[12] Under the list, Ubiquiti's 5A002 radio bridges are Tier 2 goods "Machines for the reception, conversion and transmission or regeneration of voice, images, or other data, including switching and routing apparatus." Their components include Tier 3.A. goods: an "apparatus for the transmission or reception of voice, images, or other data, including apparatus for communications in a wired or wireless network." The U.S. government flagged this category as "electronic components used in Russian weapons systems."

52. At all relevant times, these comprehensive U.S. sanctions and export controls prohibited Ubiquiti from supplying 5A002 military communications equipment to Russia and warned Ubiquiti of the risk to civilian lives if it failed to comply.

13,048, 13,048, 13,053, 13,063 (Mar. 8, 2022), https://www.govinfo.gov/content/pkg/FR-2022-03-08/pdf/2022-04819.pdf.

[11] Additions of Entities to the Entity List; Sanctions Against Russia and Belarus, 89 Fed. Reg. 4267 (Jan. 23, 2024).

[12] Bureau of Indus. & Sec., U.S. Dep't of Com., *High Priority Items List*, *supra* note 2.

III. Ubiquiti knowingly, or with willful blindness, supplies Russia with military communications equipment in violation of the export ban.

A. Ubiquiti supplies banned radio bridges to Russia through a smugglers' network of straw purchasers.

53. Since the full-scale invasion of Ukraine in February 2022, Ubiquiti has knowingly and unlawfully supplied military communications technology to Russia, through a smuggling network of distributers.

54. This network was in place during Russia's initial invasion of Crimea and eastern Ukraine in 2014.

55. On a May 8, 2014 earnings call, Ubiquiti CEO Robert Pera admitted that Ubiquiti was "monitoring" the "geopolitical issues" and continued to make "direct shipments into Ukraine or Russia."[13] When asked whether Ubiquiti has "distributors from other countries that ship into that region too," Pera admitted "we know that there's a couple other guys that more than likely move some products into Russia."

56. Ubiquiti's Russian distribution network used to operate in daylight. An archived version of the company's pre-war website prominently lists three official Russian distributors and more than a dozen resellers.[14]

57. Rather than cut off this network, Ubiquiti deleted them from its website. But behind the scenes, Ubiquiti continued to distribute products through them, concealing its role in Russia's military procurement pipeline. For the first seven months of the U.S. export ban, from March to October 2022, Ubiquiti directly shipped banned 5A002 military-communications equipment to its authorized Russian distributors, who armed the invading forces.

---

[13] Ubiquiti Inc., *Q3 2014 Earnings Call Transcript*, Discounting Cash Flows (May 8, 2014), https://discountingcashflows.com/company/UI/transcripts/2014/3/.
[14] Ubiquiti Networks, Inc., *Distributors*, Internet Archive (June 16, 2014), https://web.archive.org/web/20140616021844/http://www.ubnt.com/distributors#rusia.

58. Ubiquiti's exports to Russia should have been zero. Instead, they surged by more than 60%. In the 26 months after the export ban, the total value of Russian imports of Ubiquiti products recorded in Russian customs data was $28 million, nearly 66% higher than in the 26 months before the export ban. That excludes products not declared to customs.

59. Between February and June 2022, as Russia's need for military communications equipment grew, Ubiquiti's competitors—Cisco, Fortinet, Siemens, and HPE/Aruba—all announced their exit from the Russian market, condemning the unlawful war of aggression. But where they saw risk, Ubiquiti saw opportunity.

60. After quietly deleting its Russian distributors from its website, Ubiquiti continued to supply them through a sanctions-evasion scheme. To escape U.S. regulators, Ubiquiti routed military communications equipment through a web of authorized distributors in third countries. They acted as straw purchasers—shipping directly to Russia or forwarding through re-exporters in transshipment hubs the U.S. government has specifically flagged as high-risk for sanctions evasion, including Turkey and Kazakhstan.[15]

61. For example, one of Ubiquiti's sanctions-evasion routes went through its official Czech distributor, Discomp S.R.O. For more than two years after the invasion, Discomp shipped $1.8 million in Ubiquiti products directly to one of the authorized Russian vendors Ubiquiti had scrubbed from its website: WiFiMag. When direct shipments became too visible, Discomp rerouted the same shipments to the same client through a Turkish freight forwarder, Olimpik Gama—until the Treasury Department sanctioned Olimpik Gama in February 2024 as part of a U.S. government crackdown against "third-country facilitators" who "enable Russia to maintain,

[15] U.S. Dep't of Com., *"Red Flags" Indicative of Diversion* (Aug. 16, 2022); DOJ, BIS, & OFAC, *Tri-Seal Compliance Note: Cracking Down on Third-Party Intermediaries Used to Evade Russia-Related Sanctions and Export Controls* (Mar. 2, 2023), https://ofac.treasury.gov/media/931471/download?inline.

sustain, and rebuild its war machine." Discomp did not stop. It simply switched to a different Turkish company, Unico Tekstil, to keep the shipments to WiFiMag—and the Russian government—flowing.

62. A second example: before the invasion, Ubiquiti directly supplied three-quarters of the Ubiquiti inventory sold by Russian vendor Wireless Networks—one the Russian partners scrubbed from its website. After the invasion, the same volume of product began arriving to the same vendor, but routed through Simple Solutions, a Kazakh company with every hallmark of a shell built for straw purchasing: it was incorporated eight days after the U.S. export ban, in a town 80 miles from the Russian border; it has no public storefront or website; its registered contact email uses a Russian domain; and it shares an address with a company that advertises itself on social media as an authorized Ubiquiti reseller. Three of Ubiquiti's own authorized distributors—in Latvia, Poland, and China—supplied Simple Solutions, which sent every unit onward to Wireless Networks in Russia, who armed the Russian military.

63. This sanctions-evasion network expanded over time. In the 26 months before the export ban, a single Turkish exporter shipped roughly $195,000 in Ubiquiti products to Russia; in the 26 months after the ban, 18 Turkish re-exporters shipped nearly $3 million. Distributors and resellers in Kazakhstan, the United Arab Emirates, Hong Kong, and Kyrgyzstan began shipping Ubiquiti products to Russia for the first time only after the ban took effect, moving more than $10 million in product.

64. The last layer of Ubiquiti's sanctions-evasion network are the vendors in Russia who supply the army. Ubiquiti never stopped supplying these straw purchasers after scrubbing them from its website. As of July 2026, they still sell banned radio bridges under Ubiquiti's logo—without objection from Defendant—on Russian vendor websites like ubiquiti.ru and ubnt.ru. For

example, WiFiMag—previously an authorized reseller on Ubiquiti's website—advertises: "We are the official distributor of the manufacturer. . . . At WiFiMAG you can buy Ubiquiti Networks at low prices and in the largest assortment in Russia! . . . "

65. Ubiquiti is well-aware of these vendors—its New York headquarters scrubbed them from its website—and must be aware they are operating under its brand. In September 2025, Ubiquiti successfully registered its logo with Russia's intellectual property agency Rospatent in September 2025. The only reason to register a trademark in a country where Ubiquiti is effectively banned is because Ubiquiti is aware its logo is being used there and faces trademark dilution. By law, Ubiquiti could block that use. Instead, it is ratifying its vendors' practice of selling banned products under its brand.

66. Ubiquiti exploited this illicit smuggling scheme to supply a sizable arsenal of banned military-communication devices to the Russian military in violation of U.S. law and the Wassenaar arms-control agreement. In just the 26 months following the February 2022 invasion, Russian trade data recorded $28 million in Ubiquiti imports—a sum equivalent to more than 150,000 airMax radio bridges.[16] Since then, Ubiquiti devices continue to flow into the hands of Russian occupation forces.

67. That is just the hardware. The software updates that maintained and optimized these units were supplied directly by Ubiquiti via its website controlled from New York. For more than three years after the invasion, Ubiquiti pushed automatic firmware updates to airMAX devices operating inside Russia and Russian-occupied Ukraine—updates that kept those devices current, secure, and functioning as part of Russia's military communications infrastructure. Exporting this software and technical support also violated U.S. export controls.

[16] Most airMax radio bridges retail for less than $300 USD.

68. Only years into the conflict, in or around September 2025, did Ubiquiti stop providing firmware updates to users with Russian IP addresses—proving that Ubiquiti had the technical means to detect banned devices' location. Blocking updates does not disable a device, however. And unlike other U.S. companies, Ubiquiti has refused to disable or impair devices in Russian military hands. (*See infra* Section IV.B.)

B. Ubiquiti knows it is arming Russia with military technology "necessary to Russia's war machine"—or willfully blinds itself.

69. At all relevant times, Ubiquiti was aware of Russia's atrocities, aware its technology was dangerously enabling them, and knew or should have known it was arming Russia with battlefield communications equipment.

70. Ubiquiti was aware of Russia's invasion of Ukraine and its atrocities against Ukrainian civilians. Ubiquiti's SEC Form 10-K for each year between 2022 and 2025 admits: "We are monitoring the military conflict between Russia and Ukraine, escalating tensions in surrounding countries, and associated economic sanctions."[17] No multi-billion-dollar company monitoring the conflict could avoid knowing of Russia's well-documented war crimes and the U.S. determination that Russia was committing war crimes and crimes against humanity.

71. Ubiquiti knew that U.S. law prohibited it from exporting, reexporting, or transferring radio bridges and other 5A002 military-communications equipment to Russia. The compliance section of its website specifically flags its products as restricted 5A002 devices, including the AirMAX line of antennas and encrypted networking devices. Its SEC filings also flag that it is subject to export controls. Ubiquiti's 2022 Form 10k even discloses: "It is, however,

[17] *See, e.g.*, Ubiquiti, Form 10-K (2023) at 37, https://otp.tools.investis.com/clients/us/ubiquiti_networks_inc/SEC/sec-show.aspx?Type=html&FilingId=16889045&CIK=0001511737&Index=10000.

possible that [export control] violations may occur in the future. If violations should occur in the future, the response of regulators may be more severe in light of prior compliance concerns."

72. Ubiquiti knew that Russia needed Ubiquiti's 5A002 military-communications equipment "to sustain its aggressive military capabilities"; it knew this because U.S. authorities said so and banned them for this very reason—in export control announcements Ubiquiti could not have ignored. [18]

73. Ubiquiti knew its distributors "more than likely move some products into Russia" as its CEO Robert Pera admitted in a 2014 earnings call after the initial Russian invasion of Crimea.

74. Trade data put Ubiquiti on notice that it was funneling large volumes of banned Ubiquiti devices to Russia even after the full export ban was imposed in 2022. A 60% surge of exports to a country under embargo and condemned for crimes against humanity by the U.S. government could only be ignored through willful blindness.

75. Telemetry data directly informed Ubiquiti that large volumes of banned 5A002 radio devices were deployed in Russia, on the Russian frontlines, and in occupied-Ukraine. To receive software updates, Ubiquiti devices "phone home" to Ubiquiti's computer servers, providing telemetry data including the device's (i) geolocation information—granular to the city level—(ii) unique MAC address and serial number, and (iii) hardware model.

76. Because Ubiquiti was "monitoring the conflict," according to its SEC filings, it could not avoid knowing its banned radio bridges were deployed by the Russian military. This was open, notorious, and publicized in the Russian media.

77. Russian State television has repeatedly broadcast footage of Russian soldiers installing Ubiquiti antennas in occupied Ukraine. For example, a June 2025 video produced by the

[18] U.S. Dep't of Com., Bureau of Indus. & Sec., *Sweeping Restrictions*, *supra* note 9.

Russian Ministry of Defense shows Russian soldiers in Ukraine installing Ubiquiti LiteBeam and PowerBeam radio bridge units on a tree.

78. In another example, a July 3, 2025 report by state TV network Zvezda filmed Russian soldiers in occupied Ukraine installing a banned Ubiquiti LiteBeam antenna.

79. Online Russian vendors—operating under the Ubiquiti brand—openly market the equipment for military buyers. As one told reporters, “There are no stable, inexpensive alternatives

to this manufacturer. . . 95 percent of the shipments for the SVO [occupation of Ukraine] are Ubiquiti gear."

80. Between 2023 and 2026, Russian army units publicly linked to atrocities in Bucha, Mariupol, and Kharkiv repeatedly posted footage of Ubiquiti equipment on social media. In 2025, a Russian vendor operating ubiquiti.ru advertised a thank-you letter from a Russian military training center for supplying "wireless bridges" to soldiers fighting in Ukraine.

81. At all relevant times, Ubiquiti knew or should have known it was supplying the Russian occupation—because it was legally obligated to know its customers and monitor its distribution chain for compliance with U.S. sanctions and export controls.

82. Federal guidance set the industry standard for exactly this situation, and Ubiquiti ignored it. The U.S. Commerce Department's 2017 *Export Compliance Guidelines* instructed Ubiquiti (and other exporters) to maintain an effective compliance program with senior-management commitment.[19] It instructed Ubiquiti to know its customers and distributors—verifying a buyer's legitimacy, obtaining end-use statements, and screening every party to a transaction against U.S. proscribed-parties lists before export. It instructed Ubiquiti to treat "transshipment hubs," the very jurisdictions through which Ubiquiti's products reached Russia, as a specific and heightened diversion risk. And it instructed Ubiquiti to test their program's effectiveness through periodic internal and external audits of their distribution chain, customers, and transactions, so that vulnerabilities are caught before they ripen into violations.

83. Ubiquiti had this guidance. It did not follow it.

84. Ubiquiti has been caught doing this before. In 2014, the Treasury Department's Office of Foreign Assets Control found (i) that Ubiquiti had illegally diverted military

[19] Bureau of Indus. & Sec., U.S. Dep't of Com., *Export Compliance Guidelines: The Elements of an Effective Compliance Program* 3, 7 (Jan. 2017), https://www.bis.gov/sites/default/files/documents/ECP_0.pdf.

communication equipment to Iran through UAE distributors, that (ii) "Ubiquiti had no OFAC compliance program in place," and (iii) that "members of Ubiquiti's senior management knew or had reason to know that Ubiquiti products were reexported to Iran.[20] Ubiquiti paid $504,225 to resolve the matter. Pera publicly promised reform: "It can't happen again. If it does, I'll be in a lot of trouble."[21] It happened again.

85. Ubiquiti faced the specific, repeated red flags that the U.S. government told it to watch for in 2022.[22] Its distribution network ran through Turkey, Kazakhstan, and other transshipment points near Russia, used shell companies at residential addresses, and involved unusual corporate structures that obscured ownership and origin. BIS's "Know Your Customer" guidance—the industry standard for exactly this situation—instructs companies to investigate and resolve red flags before shipping and specifically warns: "Do not self-blind."[23]

86. Ubiquiti's New York headquarters ignored these red flags. It did so either because it was intentionally using these smugglers to evade U.S. sanctions or because it blinded itself. Aware of the high risk of arming the Russian military, it chose not to learn more, to maintain plausible deniability.

87. Ubiquiti has ample sources to run an effective compliance program. It has a market capitalization of roughly $65 billion, more than 1,600 employees, and reported $2.6 billion in revenue in 2025.

88. Instead, Ubiquiti's leadership in New York decided to cripple its compliance program, limiting it to a single position in New York, with no automated system to alert and act on

[20] OFAC, *Ubiquiti Networks, Inc. Settles Potential Civil Liability for Apparent Violations of the Iranian Transactions and Sanctions Regulations* (Mar. 6, 2014), https://ofac.treasury.gov/media/13476/download?inline.
[21] Dolan, *supra* note 1.
[22] U.S. Dep't of Com., *"Red Flags"*, *supra* note 15.
[23] 15 C.F.R. pt. 732, Supp. No. 3.

red flags. A former employee who oversaw product distribution put it plainly: "The CEO of Ubiquiti recognizes that and just doesn't care about all of the extra garbage."

89. That compliance "garbage"—which U.S. law required Ubiquiti to maintain—could have saved lives.

IV. Despite this knowledge, Ubiquiti continues to supply the Russian military and refuses to adopt commercially feasible design safeguards to protect civilians.

A. Ubiquiti refuses to cut off exposed smugglers.

90. Any reasonable exporter who learns that it is illegally arming Russian occupiers with devices "necessary to Russia's war machine," would have acted to stop the smuggling and protect civilian lives. Not Ubiquiti. Confronted with direct evidence and public accusations, it persisted.

91. On January 27, 2026, Hunterbrook, an investigative news outlet, published an exposé on Ubiquiti's role powering the Russian occupation of Ukraine.

92. The Hunterbrook report put Ubiquiti on direct, public notice that its distributors like Discomp in Czechia were key nodes in Russia's military procurement pipeline—complete with sting-verified evidence of the smuggling operations described above.

93. Ubiquiti neither denied the allegations contained in the Hunterbrook Report nor claimed that it was authorized by U.S. export licenses. Ubiquiti's own stock fell 8% that day, confirming that the market understood the report's significance.

94. Yet, as of July 25, 2026, Ubiquiti still had not terminated Discomp. No commercially reasonable company, on notice that a contractual distributor was arming an invading army committing crimes against humanity, would continue to give that distributor banned military

communication technology. Ubiquiti continues to do so, despite almost daily news reports of Russian war crimes against civilians.[24]

95. Ubiquiti retained full practical control over its distribution chain throughout this period. It could approve or terminate any distributor, demand end-user certificates, audit for diversion, and track banned devices by IP and MAC address. Its contracts gave it the right to terminate any distributor supplying Russia in violation of U.S. sanctions. It chose not to use that control. Its smuggling network remains intact, and its banned devices continue to flow into the hands of Russian occupiers.

B. Ubiquiti refuses to include kill-switch safeguards in airMAX firmware and refuses to remotely disable Russian military infrastructure.

96. Firmware is the code that lets a device start up, connect, and function. A kill switch—code that lets a manufacturer remotely disable a device—is a low-cost feature to write into firmware to prevent its criminal use by terrorists, war criminals, or national security threats.

97. Ubiquiti had already built the network-connectivity and remote-command infrastructure a kill switch requires: it already pushes remote firmware updates to its 5A002 airMAX devices based on telemetry. Writing the kill switch, and testing it, would have fit within Ubiquiti's existing firmware-update workflow at minimal cost.

98. As an added safeguard, Ubiquiti could have paired a kill switch with a whitelist, authorizing only approved device serial numbers or MAC addresses to operate in Ukraine.

99. This precise approach has been taken by other U.S. tech companies that have sought to comply with U.S. sanctions and avoid enabling Russian atrocities. SpaceX, for example, provides a global satellite internet access service called Starlink. Unlike Ubiquiti, Starlink

[24] *See, e.g.*, Andrew Kramer, *A City Where Every Step Outside Risks Death by Drone*, N.Y. Times (Jan. 28, 2026), https://www.nytimes.com/2026/01/28/world/europe/kherson-ukraine-drones-russia.html.

complied with the U.S. embargo and does not distribute devices directly to Russia. However, several years into the invasion, Russian operatives carried out a scheme to ship Starlink satellite-access terminals to western Ukraine and then divert them to Russian-occupation forces in the east.

100. Unlike Ubiquiti, SpaceX took active measures to thwart the Russian military from deploying Starlink. SpaceX uses kill-switches to block Starlink terminals whose telemetry geolocates them in Russia.

101. In late 2025, after Ukrainian officials discovered that Russia was installing Starlink terminals as navigation devices on drones flying in Ukraine, SpaceX worked with Ukraine to compile a whitelist of authorized terminals and deactivated every other Starlink terminal operating in the region through geofencing and device-ID blacklisting.[25]

102. That is proof, from a real-world deployment in the same conflict zone, that the product-design safety measures Ubiquiti refused were feasible, effective, and available to any manufacturer willing to use it.

103. Ubiquiti had every reason to know the stakes. It knew the U.S. government had branded its radio bridges "necessary to fuel Russia's war machine." It knew, from its own telemetry, that its devices were operating inside Russia and occupied Ukraine. It chose not to cut off its straw-purchasers, not to include a kill switch, not to build a whitelist, and not to disable a single device. That choice had lethal consequences.

[25] Tom Balmforth, *Ukraine Says Starlink Terminals Used by Russia Deactivated in Blow to Moscow*, Reuters (Feb. 5, 2026), https://www.reuters.com/world/europe/starlink-used-by-russian-forces-deactivated-battlefield-ukraine-says-2026-02-05/. Starlink terminals and Ubiquiti radio bridges play complementary—but not substitutable—roles in Russia's military communications infrastructure. A Starlink Terminal is a satellite internet access point; a Ubiquiti radio bridge broadcasts wireless signals connecting devices at long-range. The Ubiquiti system connects to the internet via a wired or satellite internet access point, enabling numerous military devices to share internet access.

V. The foreseeable result: Russia hunts civilians using the command-and-control system Ubiquiti supplied.

A. The "human safari."

104. The risk that Russia would deploy Ubiquiti's radio bridges against Ukrainian civilians was not merely foreseeable—it was the precise risk U.S. export controls were designed to prevent, and it materialized exactly as warned.

105. Russian forces have deployed tens of thousands of Ubiquiti devices along the annexed Provinces and the invaded border regions, linking front-line units to command posts and up the chain of command to the Ministry of Defense.

106. In modern militaries, command, control, and communications systems are "fundamental to all military operations, delivering the critical information necessary to plan, coordinate, and control forces and operations across the full range of . . . missions."[26]

107. Since the early days of the 2022 invasion, the Russian military has used Ubiquiti radio bridges to build a command-and-control system in occupied Ukraine—linking reconnaissance drones, attack units, and commanding officers through internet videoconferencing. Russian forces connect an airMAX base station to an internet access point, then extend that signal for kilometers using airMAX radio bridges, linking soldiers and drone pilots directly into the chain of command.

108. Ukrainian signals intelligence officials have concluded that Ubiquiti devices are a critical component of Russia's military communications network in Ukraine, with tens of thousands of units deployed along the front. Without a radio bridge, a Russian position becomes combat-ineffective within minutes: drone, artillery, and infantry units lose contact with

[26] U.S. Dep't of Def., *Command, Control, and Communications (C3) Modernization Strategy* (Sept. 2020), https://dodcio.defense.gov/Portals/0/Documents/DoD-C3-Strategy.pdf.

reconnaissance and command and cannot deliver coordinated fire. That is why Ukrainian forces target the antennas relentlessly—and why Russia keeps replacing them with a seemingly inexhaustible supply.

109. On July 3, 2025, the Russian Ministry of Defense credited Ubiquiti radio bridges for making the invasion of Ukraine possible. In a State Television broadcast showing the military deployment of Ubiquiti antennas, the Ministry stated: "The use of wireless broadband technologies has significantly increased the effectiveness of unit command and control by providing commanders with reliable and secure communications. The solution is especially relevant in the context of the special military operation [*i.e.*, occupation of Ukraine] where traditional methods of organizing communications cannot always be implemented quickly."[27]

110. On social media, Russian forces routinely praise Ubiquiti's products for helping the occupation. A video posted online by Russian soldiers posing in a trench with Ubiquiti products gave thanks to Ubiquiti suppliers, stating: "We thank the People's Militia Assistance Group for providing military communications equipment in the form of Ubiquiti antennas. No communication, no front. The old military saying is truer than ever."

111. Russian forces have used Ubiquiti devices to maintain a "kill zone" extending up to 100 kilometers behind the front lines blanketed with reconnaissance drones and sensors under constant surveillance. Anything that moves is caught on camera and streamed on Russia's command-and-control videoconference network where targets are selected, kills are confirmed, and trophy videos are disseminated in a deadly feedback loop. This command-and-control system—and the kill zone it enables—would be impossible without Ubiquiti radio bridges.

---

[27] TASS, *Связисты "Запада" развернули уникальную систему беспроводной связи в зоне СВО* [Signal Troops of the "West" Group Deployed a Unique Wireless Communications System in the Zone of Special Military Operation], TASS (July 3, 2025), https://tass.ru/armiya-i-opk/24416841.

112. Since at least January 2024, Russian forces have carried out a widespread, systematic campaign of drone and drone-assisted attacks on civilians in the kill zone—watching roads, gardens, and homes from reconnaissance drones and launching artillery or directing first-person-view ("FPV") attack drones, small enough to chase a person through an open door, to kill on command.[28] The campaign is called the "human safari."

113. Russia launched the human safari in Kherson city, in southeastern Ukraine in the early 2024. By July 2026, the human safari has spread throughout the 100 km kill zone (sometimes called a "red zone") that stretches like a scar across Ukraine, from the Black Sea to the northern Russian border.

114. Russian social media channels tied to the units carrying out these strikes broadcast the campaign's own name and purpose in their captions: "Civilians moving in the red zone do so at their own risk, by definition, any movement is a target." "Once again. Everything that moves will be destroyed."

115. A Ukrainian signals officer explained why the human safari depends on the Ubiquiti-enabled command-and-control system: "The FPV [drone] unit is unable to work without aerial reconnaissance; they'd be flying blind."

116. Russia's human safari campaign has been widely reported in the U.S. and international media, and documented by United Nations investigators, who characterize it as a

[28] Human Rights Watch, *Listen, Run, Hide: How Russia Uses Quadcopter Drones to Hunt and Kill Civilians in Kherson, Ukraine* (June 3, 2025), https://www.hrw.org/feature/2025/06/03/listen-run-hide/how-russia-uses-quadcopter-drones-hunt-kill-kherson.

crime against humanity.[29] The campaign has deprived thousands of Ukrainian civilians of the safe use of public roads and spaces. As a limited countermeasure, streets in urban centers are draped in nets to try to catch drones.[30]

Drone nets cover the streets of Izium, Ukraine, on Feb. 7. The netting discourages drones from diving at cars and people because their propellers get tangled in it.
Anton Shtuka for NPR

B. The attack on the Kovalenko family.

117. In the summer of 2024, Plaintiff Diana Kovalenko and her husband Max Kovalenko were prominent doctors in Kherson Province, Ukraine. They lived in the Antonivka suburb of Kherson, near the right bank of the Dnipro River. Their adult son, Plaintiff Taras Kovalenko, also a doctor, had a home in the same neighborhood near his parents.

[29] *See, e.g.*, UN High Commissioner for Human Rights, Press Release, *UN Commission concludes that Russian armed forces' drone attacks against civilians in Kherson Province amount to crimes against humanity of murder*, May 28, 2025, https://www.ohchr.org/en/press-releases/2025/05/un-commission-concludes-russian-armed-forces-drone-attacks-against-civilians; Andrew E. Kramer, *Russia Aims Drone Attacks at Civilians, a War Crime, U.N. Inquiry Says*, N.Y. Times, Oct. 27, 2025, https://www.nytimes.com/2025/10/27/world/europe/russia-drones-target-civilians.html.
[30] Eleanor Beardsley, *Ukraine Strings Nets over Cities as Killer Drones Turn Streets into War Zones*, NPR (Mar. 17, 2026), https://www.npr.org/2026/03/17/nx-s1-5743446/russia-ukraine-war-nets-drones

118. The Kovalenkos' neighborhood came under constant surveillance and attack by drones launched by Russian occupation forces, who were commanded and controlled through the Ubiquiti radio bridge system. As the daily human safari escalated, the Kovalenkos were forced to abandon their homes.

119. On September 2, 2024, Max and Diana briefly returned home to gather clothes for the winter.

120. On the other bank of the Dnipro River, Russian forces, deployed through the Ubiquiti enabled command-and-control system, launched an FPV drone to stalk their neighborhood. They were based within 5 km of the Kovalenkos.

121. As Max and Diana drove back, the Russian FPV drone tracked their car and dropped an explosive through the windshield, livestreaming the attack on video. Later that day, Russian soldiers posted the trophy video on the Telegram social media app. The video shows the

sequence of the murder: crosshairs track a civilian vehicle, a green bomb is released, a fiery blast, then a round hole appears in the windshield directly above the driver.

122. The caption of the video states: "Kherson. Red Zone. […] We also want to highlight the skill of the operator working at the highest point while on the move. His precision, and most importantly, the quality of his execution, are top-notch. With each passing day, our hunters' work becomes more and more effective, which means the goal of liberating Kherson from the Nazi rabble is getting closer and closer."

123. After the blast, Diana blacked out in the passenger seat. When she came to, she was covered in shattered glass and blood. Shrapnel had mangled her right eye and pierced her left hand, left breast, and lungs. Max was not breathing; she saw blood pouring out of a hole in his chest. Neighbors rushed them to a hospital. Max was pronounced dead.

124. Neither Max nor Diana were combatants and there were no military targets in the vicinity of the attack.

125. Their son, Taras, drove from Western Ukraine to come to their aid. He brought Diana to a secure location in Western Ukraine, where she remains internally displaced, unable to work as a doctor, and suffering from ongoing physical pain and emotional trauma.

126. Since the attack, Diana returned only once to Kherson to visit Max's grave. But she cannot safely return to her home in Antonivka. Her neighborhood is a ghost town. Most neighbors have also fled. The drones circle above and there is a constant threat of attack.

127. Taras experienced this threat firsthand. When he came to visit his father's grave, he was forced to run for his life and hide under a tree when a Russian hunter drone came stalking the cemetery.

C. The attack on Anatoliy Savchenko.

128. In the fall of 2025, Anatoliy Savchenko was working for a private energy company in Chernihiv Province. The Chernihiv region was under constant surveillance and attack by drones launched by Russian occupation forces, who were commanded and controlled through the Ubiquiti radio bridge system.

129. On the evening of October 10, 2025, Anatoliy was driving back from a job near the village of Zhadove, roughly 22 km from the Russian border. Suddenly, his automobile was targeted by a Russian drone. A second crew of engineers, traveling several minutes behind, arrived to find the car on fire. Anatoliy was lying on the ground, wounded but alive and unable to walk. As his colleagues lifted him up to load him in their car, a second Russian drone arrived in a "double-tap" attack on the rescuers. The drone exploded into the group of workers, killing Anatoliy, and injuring others.

130. None of the victims were combatants and there were no military targets in the vicinity of the attack.

131. Anatoliy's body laid out by the road all night. It was unsafe to recover his remains: the drones returned throughout the night, stalking anyone who moved.

132. The next morning, his wife, Liubov Savchenko and her son, V.S., were informed that Anatoliy was dead. They suffer ongoing emotional trauma and distress.

133. Like all the other civilians in the kill zone, Liubov and V.S. live under the constant threat of Russian drones buzzing through the air. The hunter drones are still a daily reality in Chernihiv Province, and they live in fear of the human safari.

D. The attack on Vasyl Shestak.

134. In September 2025, Vasyl Shestak was working as a fireman in the village of Kostobobriv in Chernihiv Province, located less than 2 km from the Russian border and within the Russian kill zone.

135. Russian forces placed the Kostobobriv region under constant drone surveillance and attack by drones launched by units commanded and controlled through the Ubiquiti radio bridge system.

136. Mr. Shestak's fire department was routinely pursued and attacked by Russian FPV drones.

137. On or about September 13, 2025, Vasyl received a call for help from a friend whose home in Kostobobriv was under attack by drones. Vasyl came to his aid but soon became a target himself. An FPV quadcopter drone with attached explosives was buzzing low above the ground. He hid under an apricot tree, then made a run for his friend's house to take shelter. The drone whirred after him. Just as Vasyl started climbing the porch, the drone launched its explosives meters away from him. The blast tore a hole in his ribs. He watched the drone approach and hover over him for 30 seconds, its camera trained on him. He played dead until the drone flew away, heading back in the direction of the Russian border. He was rushed to a hospital and as the adrenaline wore off, felt the searing pain of his wound. Shrapnel had fractured a rib and pierced several internal organs.

138. None of the victims were combatants and there were no military targets in the vicinity of the attack.

139. Vasyl experiences ongoing physical and emotional pain and suffering and is unable to work as a first responder. The hunter drones are still a daily reality and Vasyl lives in fear of the human safari.

E. The attack on Valerii and Olena Kobylianskyi

140. In the summer of 2025, married couple Valerii Kobylianskyi and Olena Kobylianska were working at the Semenivka section of the Koriukivka District Power Grid in Ukraine's Chernihiv region, a civilian electricity facility located less than 20 km from the Russian border, within the kill zone.

141. The Chernihiv region was placed under constant surveillance and attack by drones launched by Russian occupation forces, who were commanded and controlled through the Ubiquiti radio bridge system.

142. On or about August 12, 2025, a Russian FPV drone tracked Valerii's vehicle as he entered the parking lot of the electrical station. As he exited the vehicle, the drone slammed into the ground nearby, detonating an explosive and sending shrapnel flying. Valerii fell to the ground, his body pierced by fragments.

143. Olena was working inside, with a view of the parking lot from her office. When the drone struck, the blast wave shattered the glass window. She heard screams and ran outside. In horror, she saw her husband Valerii on the ground and believed he was dead. She called an ambulance and administered first aid to her husband.

144. Valerii was taken to a hospital, where surgeons attempted to remove shrapnel from his hip and leg. They could not remove shrapnel embedded in his pelvis because the risk of paralysis was too great. He was also treated for traumatic brain injury.

145. To this day, Valerii suffers severe physical pain and emotional trauma. Olena endured severe emotional trauma from surviving the attack and witnessing her husband's injuries.

146. None of the victims were combatants and there were no military targets in the vicinity of the attack.

147. The hunter drones are still a daily reality and Valerii and Olena live in fear of the human safari.

F. The attack on the Tsylinko Family

148. In May 2026, Svitlana was living in Kherson City, Ukraine with her minor son, D., and her mother. Svitlana was on maternity leave, but still formally employed as a postal-service operator.

149. Kherson is under constant drone surveillance and attack by drones launched by Russian units commanded and controlled through the Ubiquiti radio bridge system.

150. On or about May 27, 2026, Svitlana and her seven-year-old son D.T. were on their balcony watering flowers while Svitlana's mother was in the kitchen. Suddenly, a Russian drone struck the courtyard of the apartment, which was one of three near-simultaneous impacts in the area. The blast shattered the windows of Svitlana's apartment and threw her and D.T. several meters back from the balcony, slamming them to the floor inside the apartment. Svitlana landed on her side and hip and D.T. fell onto his back and struck his head.

151. Svitlana's right leg was injured and she sustained a blast barotrauma. D. sustained a concussion and an acute stress reaction. They were temporarily deafened by the strike.

152. None of the victims were combatants and there were no military targets in the vicinity of the attack.

153. Svitlana and D.T continue to suffer from ongoing physical pain and emotional trauma.

CHOICE OF LAW

154. *Conduct-Regulating Rules*: New York tort law governs all conduct-regulating rules, including the standards of care and elements of negligence, products liability, and intentional torts. *Licci ex rel. Licci v. Lebanese Canadian Bank, SAL*, 739 F.3d 45, 50–51 (2d Cir. 2013).

155. New York is the *situs* of Ubiquiti's wrongful conduct, and New York has the greatest interest in regulating the conduct of companies within its borders and creating consistent business expectations. Ubiquiti's decisions to maintain and conceal its Russian distribution channel, to gut its own compliance function, and to design airMAX firmware without a kill switch were all made from Ubiquiti's headquarters in New York.

156. In addition, New York has expressly declared a public policy against allowing its residents and resources to support Russia's war on Ukraine. On February 27, 2022, Governor Hochul's Executive Order No. 14 directed state divestment from any entity supporting Russia's invasion, declaring that New York "strongly condemns Russia's actions against Ukraine" and "will not permit its own investment activity, whether directly or indirectly, to aid Russia . . . as it commits these human rights violations and atrocities . . . ."

157. New York, therefore, has a compelling interest in applying its conduct-regulating rules to the conduct of companies like Ubiquiti that flout compliance obligations and provide support to the Russian government's human rights atrocities from within New York.

158. *Loss-Allocating Rules*: Ukrainian law governs "all post-event tort loss-distribution questions" because the parties do not share the same domicile and because the deaths and injuries occurred in Ukraine, Plaintiffs' domicile. *Licci*, 739 F.3d at 49 (citation modified). Regulations and restrictions on damages recoverable from a wrongful death, and who may recover them, are loss-allocating rules. *See id.*; *Barkanic v. Gen. Admin. of Civ. Aviation of the People's Republic of China*, 923 F.2d 957, 962–3 (2d Cir. 1991) (applying *Neumeier v. Kuehner*, 31 N.Y.2d 121, 128 (1972)).

159. Under Ukrainian law, Plaintiffs Diana and Taras Kovalenko and Liubov and V. Savchenko are proper wrongful death claimants, entitled to recover economic and non-economic damages (moral damages) caused by the loss of their respective spouses and fathers.

160. Article 1168 of the Ukrainian Civil Code ("UCC") provides that, in the event of a wrongful death, moral (non-pecuniary) damages are limited to the decedents' "spouse, parents (adoptive parents), children (adopted), as well as persons who lived with him/her in the same family."

161. Under Chapter 87, Art. 1269 UCC, an individual may "exercise . . . the right to inheritance" if he or she either (i) accepts the inheritance within six months, or other time provided by Art. 1270; (ii) is a minor, and thus, deemed to have accepted the inheritance under Art. 1268(4); or (iii) permanently resided with the decedent at the time of death and has not renounced the inheritance.

162. Under the rules of intestate succession, the heirs at law are entitled to equal shares, Art. 1267(1), among the decedent's children, surviving spouse, and parents, Articles 1258, 1261(1), or in the absence of those heirs, to siblings and grandparents, Art. 1262(1).

WARTIME TOLLING

163. All of Plaintiffs' claims are timely. NY CPLR § 209 tolls the statute of limitations for claims arising in, or in territory occupied by, a country at war with the United States or its allies, until hostilities end. Russia has occupied Ukraine since its February 24, 2022 invasion, and Ubiquiti's products caused Plaintiffs' injuries from Russian or Russian-occupied territory and within the 100 km "kill zone" which occupying Russian forces have imposed through drones.

164. Ukraine is a U.S. ally at war with Russia for purposes of § 209. The United States and Ukraine entered into the November 2021 Charter on Strategic Partnership mutually committing to "countering Russia's aggression," "defense and security cooperation," and

"intelligence sharing"[31] and by the June 2024 Bilateral Security Agreement, making "security-related commitments . . . intended to support Ukraine's efforts to win today's war and deter future Russian military aggression."[32] To implement these defense agreements, the United States revived Lend-Lease, a World War II-era measure that allowed the U.S. to quickly supply allied states at war with Nazi Germany.[33] Since February 2022, the United States has committed more than $64 billion in defense assistance to Ukraine—the largest sustained U.S. military aid effort since World War II.[34]

165. All claims are timely under Ukrainian law for purposes of NY CPLR § 202. Article 257 UCC provides for a three-year statute of limitations for tort claims. Ukraine suspended this statute of limitations between March 17, 2022 and September 3, 2025. Law No. 4434-IX (May 14, 2025); "Final and transitional provision", ¶ 19, UCC. Claims accruing during that period must be filed by September 3, 2028.

CAUSES OF ACTION

COUNT ONE — NEGLIGENT ENTRUSTMENT

All Plaintiffs

166. Plaintiffs incorporate all allegations set forth in paragraphs 1–165.

167. Under New York law, a supplier who entrusts a dangerous instrumentality to someone it knows, or has reason to know, is likely to use it in a manner causing unreasonable risk

[31] State Dep't., *U.S.-Ukraine Charter on Strategic Partnership* (Nov. 10, 2021), https://2021-2025.state.gov/u-s-ukraine-charter-on-strategic-partnership/.
[32] The White House, *Bilateral Security Agreement Between the United States of America and Ukraine*, June 13, 2024, *available at* https://web.archive.org/web/20240613193405/https://www.whitehouse.gov/briefing-room/statements-releases/2024/06/13/bilateral-security-agreement-between-the-united-states-of-america-and-ukraine/ [archived].
[33] Andrew Desiderio, *In the Fight Against Putin, Senate Unanimously Approves Measure That Once Helped Beat Hitler*, Politico (Apr. 6, 2022), https://www.politico.com/news/2022/04/06/senate-unanimously-approves-lend-lease-00023668.
[34] Jonathan Masters & Will Merrow, *Here's How Much Aid the United States Has Sent Ukraine*, Council on Foreign Rels. (updated Feb. 23, 2026), https://www.cfr.org/articles/how-much-us-aid-going-ukraine/.

of harm is liable for the resulting harm. That duty extends through successive, reasonably anticipated entrustees. And it reaches a manufacturer that distributes to a straw purchaser it knows or should know is trafficking into a criminal market.

168. The U.S. government repeatedly put Ubiquiti on notice that its 5A002 radio bridges were dangerous instrumentalities that Russia "needs to sustain its brutal attack on Ukraine" and that are "used in Russian weapons systems."[35]

169. Ubiquiti nonetheless continued, directly and through its distribution network, to supply large volumes of radio bridges and firmware to Russia. Ubiquiti disregarded repeated red flags that its distributors and resellers were smuggling products to the Russian military and that the Russian military was deploying those products against Ukrainian civilians in its brutal occupation.

170. Ubiquiti had the practical ability to monitor and control its distribution channel, to terminate distributors evading sanctions, and to disable devices it could see operating in Russia through telemetry. It did none of these things—in contrast to other U.S. tech companies.

171. It was foreseeable that Russia's military would deploy these radio bridges against Ukrainian civilians—that is precisely the harm the sanctions and export controls were designed to prevent. The human safari that harmed Plaintiffs and their loved ones was organized and carried out through the Ubiquiti-enabled command-and-control system described above. Ubiquiti's entrustment of radio bridges and firmware to the Russian military was thus a substantial factor in the human safari attacks that harmed Plaintiffs.

172. As a direct and proximate result of Defendant's conduct, Plaintiff Diana Kovalenko suffered severe physical injuries and emotional distress from the human safari campaign and the

[35] Bureau of Indus. & Sec., U.S. Dep't of Com., *High Priority Items List*, *supra* note 2.

murder of Max Kovalenko. She is entitled to compensatory economic and non-economic damages in amounts to be determined at trial.

173. As a direct and proximate result of Defendant's conduct, Plaintiff Taras Kovalenko suffered severe emotional distress from the murder of Max Kovalenko and from being terrorized by the human safari campaign. He is entitled to compensatory economic and non-economic damages in amounts to be determined at trial.

174. As a direct and proximate result of Defendant's conduct, Plaintiff Liubov Savchenko and her minor son, V.S., suffered severe emotional distress from the murder of Anatoliy Savchenko and from being terrorized by the human safari campaign. They are entitled to compensatory economic and non-economic damages in amounts to be determined at trial.

175. As a direct and proximate result of Defendant's conduct, Plaintiff Vasyl Shestak suffered severe physical injuries and emotional distress from the human safari campaign and is entitled to compensatory economic and non-economic damages in amounts to be determined at trial.

176. As a direct and proximate result of Defendant's conduct, Plaintiff Valerii Kobylianksyi suffered severe physical injuries and emotional distress from the human safari campaign and is entitled to compensatory economic and non-economic damages in amounts to be determined at trial.

177. As a direct and proximate result of Defendant's conduct, Plaintiff Olena Kobylianksyi suffered severe emotional distress from the human safari campaign and is entitled to compensatory economic and non-economic damages in amounts to be determined at trial.

178. As a direct and proximate result of Defendant's conduct, Plaintiff Svitlana Tsylinko and her minor son, D.T., suffered severe physical injuries and emotional distress from the human

safari campaign and are entitled to compensatory economic and non-economic damages in amounts to be determined at trial.

179. Ubiquiti's conduct was grossly negligent and wantonly and recklessly indifferent to the rights of others: it defied specific government warnings, consciously disregarded known red flags of sanctions evasion, and directly serviced Russia's command and control system. All Plaintiffs are entitled to punitive damages.

COUNT TWO — PUBLIC NUISANCE

All Plaintiffs

180. Plaintiffs incorporate all allegations set forth in paragraphs 1–165.

181. Under New York law, a public nuisance claim lies against a manufacturer that supplies a dangerous product to criminal end users, directly or through a foreseeable intermediary, and knew or should have known of their dangerous propensity.

182. From its New York headquarters, Ubiquiti knowingly, recklessly, or negligently caused, contributed to, or maintained a public nuisance by supplying critical military communications infrastructure to the Russian military in violation of U.S. export controls and its own compliance obligations. That infrastructure contributed to or maintained Russia's human safari, which constitutes a public nuisance under New York law: conduct that interferes with rights common to the public and endangers the health, safety, and property of a considerable number of persons.

183. As a result, civilians within the 100 km kill zone—including Plaintiffs—could not safely use public roads, parks, and cemeteries, and thousands have been displaced from their homes.

184. Plaintiffs suffered special injury distinct from the general public: physical harm or the death of a spouse, parent, child, or family-household member.

185. Ubiquiti's conduct was a substantial factor in the human safari attacks that harmed Plaintiffs and/or killed their relatives.

186. Plaintiffs incorporate the compensatory and punitive damages allegations set forth above in paragraphs 172–179.

COUNT THREE – STRICT PRODUCT LIABILITY (DESIGN DEFECT)

All Plaintiffs

187. Plaintiffs incorporate all allegations set forth in paragraphs 1–165.

188. As designed, Ubiquiti's airMAX radio bridges and firmware were not reasonably safe. They are export-controlled devices with military applications and a foreseeable capacity to cause mass civilian harm, yet Ubiquiti built them with no kill switch and no whitelist to prevent their use by a sanctioned military end-user.

189. A safer design was feasible: Ubiquiti already had the remote-update infrastructure that a kill switch or whitelist requires, and SpaceX's 2026 Starlink shutdown proves such a design works in this exact theater of war. The risk of harm was not speculative—the Commerce Department had designated this category of device critical to Russia's war machine, the Russian Ministry of Defense had publicly praised it, and Ubiquiti's own telemetry confirmed the deployment. Given this concrete and foreseeable risk to human life, the burden of programming a kill switch or whitelist was slight.

190. Ubiquiti's defective design was a substantial factor in the human safari attacks that harmed Plaintiffs and/or killed their relatives.

191. Plaintiffs incorporate the compensatory and punitive damages allegations set forth above in paragraphs 172–179.

COUNT FOUR — NEGLIGENT PRODUCT DESIGN

All Plaintiffs

192. Plaintiffs incorporate all allegations set forth in paragraphs 1–165.

193. A kill switch or whitelist would have had minimal impact on the utility of airMAX devices to lawful users, particularly since Russian end-users were already banned from lawfully acquiring them. That marginal cost is far outweighed by the foreseeable risk that Ubiquiti's own distribution network would put these devices in the hands of the Russian military. A reasonable manufacturer would have concluded that the risk of omitting these safeguards outweighed their minimal cost.

194. Ubiquiti's unreasonable design choices were a substantial factor in the human safari attacks that harmed Plaintiffs and/or killed their relatives.

195. Plaintiffs incorporate the compensatory and punitive damages allegations set forth above in paragraphs 172–179.

COUNT FIVE — NEGLIGENT INFLICTION OF EMOTIONAL DISTRESS

Plaintiffs Diana Kovalenko and Olena Kobylianska

196. Plaintiffs incorporate all allegations set forth in paragraphs 1–165.

197. As alleged above, Defendant's negligent conduct created an unreasonable risk of bodily harm to Plaintiffs Diana Kovalenko and Olena Koblyianskyi.

198. Defendant's conduct was a substantial factor in causing the injury and death of Diana Kovalenko's husband Max, which she observed contemporaneously, and the injury of Olena Koblyianskyi's husband Valerii, which she observed contemporaneously.

199. As a direct and proximate result, both Plaintiffs suffered severe emotional distress.

200. Plaintiffs Diana Kovalenko and Olena Kobylianska incorporate the compensatory and punitive damages allegations set forth in Paragraphs 172–179 relating to their emotional distress.

COUNT SIX — AIDING AND ABETTING ASSAULT

Plaintiffs Diana Kovalenko, Taras Kovalenko, Vasyl Shestak, Valerii Kobylianskyi, Olena Kobylianska, Svitlana Tsylinko, and D.T.

201. Plaintiffs incorporate all allegations set forth in paragraphs 1–165.

202. Under New York law, "[a]n aiding and abetting cause of action must allege facts giving rise to a strong inference that the defendant actually knew of the underlying harm or was wilfully blind to it, and rendered substantial assistance, including concealing, or failing to act when required to do so, enabling the harm to proceed . . . ." *Sayles v. Ferone*, 137 A.D.3d 486 (N.Y. App. Div. 2016). The claim has three elements: "(1) the existence of a violation by the primary (as opposed to the aiding and abetting) party; (2) knowledge of this violation on the part of the aider and abettor; and (3) substantial assistance by the aider and abettor in the achievement of the primary violation." *Design Strategy, Inc. v. Davis*, 469 F.3d 284, 303 (2d Cir. 2006) (citation modified).

203. Russian military forces committed assaults by using the Ubiquiti-enabled command-and-control system to carry out a human safari campaign that subjected Plaintiffs to fear of imminent drone strikes.

204. Ubiquiti had actual knowledge of Russia's invasion and its atrocities since at least 2014. And it had specific U.S.-government warnings since 2022 that Russia posed "an immediate danger to those living in Ukraine" and that Ubiquiti's radio bridges were banned military devices, dangerous in Russian hands, and used in Russian weapon systems.[36] Defendant knew that a substantial portion of Ubiquiti's distribution channel operated in high-risk transshipment points. It knew a substantial share of its distribution network ran through high-risk transshipment points, and it knew Russian resellers—using its own logo—were selling smuggled Ubiquiti products while it quietly scrubbed them from its own website. It knew from telemetry data that banned devices were being used in Russia and occupied Ukraine and it could not avoid knowing that the Russian military was openly and notoriously using—and praising—its devices as instrumental to the occupation.

205. In the alternative, by gutting the compliance function it was legally obligated to maintain, Ubiquiti willfully blinded itself to the fact that it was supplying banned military communications to Russia, directly or through distributors, and that these devices were deployed against Ukrainian civilians, enabling the occupation and human safari campaign.

206. Ubiquiti gave substantial, culpable assistance to the human safari campaign by supplying critical military communications infrastructure—radio bridges and firmware—in violation of U.S. export controls, on a scale and at a frequency necessary to sustain that campaign despite being warned by U.S. authorities that its 5A002 devices were "technologies" Russia "needs to sustain its brutal attack on Ukraine."[37]

[36] U.S. Dep't of Com., Bureau of Indus. & Sec., *Sweeping Restrictions*, *supra* note 9.
[37] Bureau of Indus. & Sec., U.S. Dep't of Com., *High Priority Items List, supra* note 2; U.S. Gov't Accountability Off., *supra* note 6.

207. That assistance was a substantial factor in the human safari campaign that subjected Plaintiffs to assaults.

208. Plaintiffs Diana Kovalenko, Taras Kovalenko, Vasyl Shestak, Valerii Kobylianskyi, Olena Kobylianska, Svitlana Tsylinko, and D.T. incorporate the compensatory and punitive damages allegations set forth in Paragraphs 172–179 relating to their assaults.

COUNT SEVEN – AIDING AND ABETTING BATTERY

Plaintiffs Diana Kovalenko, Taras Kovalenko, Valerii Kobylianskyi, Liubov Savchenko, V.S., Vasyl Shestak, Svitlana Tsylinko, and D.T.

209. Plaintiffs incorporate all allegations set forth in paragraphs 1–165.

210. Russian military forces committed battery by using the Ubiquiti-enabled command-and-control system to carry out a human safari campaign that subjected Plaintiffs to harmful physical contact or killed Plaintiffs' relatives by drone and drone-assisted strikes.

211. As alleged above, Ubiquiti provided substantial, culpable assistance to Russia, with knowledge or willfulness blindness, and this assistance was a substantial factor in the human safari campaign that physically injured Plaintiffs and/or killed their relatives.

212. Plaintiffs Diana Kovalenko, Taras Kovalenko, Valerii Kobylianskyi, Liubov Savchenko, V.S., Vasyl Shestak, Svitlana Tsylinko, and D.T. incorporate the compensatory and punitive damages allegations set forth above in Paragraphs 172–179 relating to their batteries.

COUNT EIGHT – AIDING AND ABETTING INTENTIONAL INFLICTION OF EMOTIONAL DISTRESS

All Plaintiffs

213. Plaintiffs incorporate all allegations set forth in paragraphs 1–165.

214. The Russian military committed intentional infliction of emotional distress by subjecting Plaintiffs to the human safari campaign—conduct so outrageous and extreme that it exceeds all bounds of decency tolerated in a civilized community.

215. Ubiquiti knew of Russia's invasion and its attacks on civilians, knew its radio bridges were necessary to sustain Russia's war effort, and knew that supply them to Russia in violation of U.S. sanctions would contribute to attacks like those on Plaintiffs. Ubiquiti substantially contributed to the command-and-control system Russia used to carry out that campaign against Plaintiffs.

216. Plaintiffs incorporate the compensatory and punitive damages allegations set forth above in paragraphs 172–179.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request that the Court enter judgment in favor of Plaintiffs against Defendant Ubiquiti, Inc., and:

a. Order Ubiquiti to abate the public nuisance and other dangers posed to Plaintiffs by its products by incorporating into airMax or other necessary software a kill switch and white-list functionality, or other appropriate design mechanism, to remotely disable unauthorized airMax devices from being used in Russia and Russian-occupied Ukraine;

b. Order Ubiquiti to pay compensatory damages exceeding $75,000,000, in an amount to be determined at trial;

c. Order Ubiquiti to pay punitive damages in an amount to be determined at trial;

d. Order Ubiquiti to pay attorneys' fees and costs of suit;

e. Order Ubiquiti to pay both pre- and post-judgment interest on any amounts awarded; and

f. Order all other relief the Court deems just and proper.

JURY TRIAL DEMAND

Plaintiffs hereby demand a trial by jury on all issues so triable.

Dated: August 11, 2026

/s/ Greg G. Gutzler
Greg G. Gutzler
Emma L. Bruder
DiCELLO LEVITT LLP
485 Lexington Avenue, Suite 1001
New York, NY 10017
(646) 933-1000
ggutzler@dicellolevitt.com
ebruder@dicellolevitt.com

Scott A. Gilmore*
DiCELLO LEVITT LLP
801 17th Street, NW, Suite 430
Washington, DC 20006
Tel: (202) 975-2288
sgilmore@dicellolevitt.com

Adam J. Levitt
DiCELLO LEVITT LLP
Ten North Dearborn Street, Sixth Floor
Chicago, Illinois 60602
Tel.: (312) 214-7900
alevitt@dicellolevitt.com

Mark A. DiCello*
Robert F. DiCello*
Kenneth Abbarno*
DiCELLO LEVITT LLP
8160 Norton Parkway
Mentor, OH 44060
Tel.: (440) 953-8888
madicello@dicellolevitt.com

rfdicello@dicellolevitt.com
kabbarno@dicellolevitt.com

* *pro hoc vice* forthcoming

Counsel for the Plaintiffs