Artificial intelligence (AI) mass surveillance at Paris Olympics – a legal scholar on the security boon and privacy nightmare

Monday 5 August 2024, by McKENNA Anne Toomey (Date first published: 17 July 2024).

Contents

The 2024 Paris Olympics is drawing the eyes of the world as thousands of athletes and support personnel and hundreds of thousands of visitors from around the globe converge in France. It's not just the eyes of the world that will be watching. Artificial intelligence systems will be watching, too.

Government and private companies will be using advanced AI tools and other surveillance tech to conduct pervasive and persistent surveillance before, during and after the Games. The Olympic world stage and international crowds pose increased security risks so significant that in recent years authorities and critics have described the Olympics as the "world's largest security operations outside of war."

The French government, hand in hand with the private tech sector, has harnessed that legitimate need for increased security as grounds to deploy technologically advanced surveillance and data gathering tools. Its surveillance plans to meet those risks, including controversial use of experimental AI video surveillance, are so extensive that the country had to change its laws to make the planned surveillance legal.

The plan goes beyond new AI video surveillance systems. According to news reports, the prime minister's office has negotiated a provisional decree that is classified to permit the government to significantly ramp up traditional, surreptitious surveillance and information gathering tools for the duration of the Games. These include wiretapping; collecting geolocation, communications and computer data; and capturing greater amounts of visual and audio data.

French President Emmanuel Macron reviews surveillance cameras in preparation for the Paris Olympics. Christophe Petit Tesson/AFP via Getty Images

I am a law professor and attorney, and I research, teach and write about privacy, artificial intelligence and surveillance. I also provide legal and policy guidance on these subjects to legislators and others. Increased security risks can and do require increased surveillance. This year, France has faced concerns about its Olympic security capabilities and credible threats around public sporting events.

Preventive measures should be proportional to the risks, however. Globally, critics claim that France is using the Olympics as a surveillance power grab and that the government will use this "exceptional" surveillance justification to normalize society-wide state surveillance.

At the same time, there are legitimate concerns about adequate and effective surveillance for security. In the U.S., for example, the nation is asking how the Secret Service's security surveillance failed to prevent an assassination attempt on former President Donald Trump on July 13, 2024.

AI-powered mass surveillance

Enabled by newly expanded surveillance laws, French authorities have been working with AI companies Videtics, Orange Business, ChapsVision and Wintics to deploy sweeping AI video surveillance. They have used the AI surveillance during major concerts, sporting events and in metro and train stations during heavy use periods, including around a Taylor Swift concert and the Cannes Film Festival. French officials said these AI surveillance experiments went well and the "lights are green" for future uses.

The AI software in use is generally designed to flag certain events like changes in crowd size and movement, abandoned objects, the presence or use of weapons, a body on the ground, smoke or flames, and certain traffic violations. The goal is for the the surveillance systems to immediately, in real time, detect events like a crowd surging toward a gate or a person leaving a backpack on a crowded street corner and alert security personnel. Flagging these events seems like a logical and sensible use of technology.

But the real privacy and legal questions flow from how these systems function and are being used. How much and what types of data have to be collected and analyzed to flag these events? What are the systems' training data, error rates and evidence of bias or inaccuracy? What is done with the data after it is collected, and who has access to it? There's little in the way of transparency to answer these questions. Despite safeguards aimed at preventing the use of biometric data that can identify people, it's possible the training data captures this information and the systems could be adjusted to use it.

By giving these private companies access to thousands of video cameras already located throughout France, harnessing and coordinating the surveillance capabilities of rail companies and transport operators, and allowing the use of drones with cameras, France is legally permitting and supporting these companies to test and train AI software on its citizens and visitors.

Legalized mass surveillance

Both the need for and the practice of government surveillance at the Olympics is nothing new. Security and privacy concerns at the 2022 Winter Olympics in Beijing were so high that the FBI urged "all athletes" to leave personal cellphones at home and only use a burner phone while in China because of the extreme level of government surveillance.

France, however, is a member state of the European Union. The EU's General Data Protection Regulation is one of the strongest data privacy laws in the world, and the EU's AI Act is leading efforts to regulate harmful uses of AI technologies. As a member of the EU, France must follow EU law.

Video: France has cleared the way legally to expand its use of AI in surveillance of public places.

Preparing for the Olympics, France in 2023 enacted Law No. 2023-380, a package of laws to provide a legal framework for the 2024 Olympics. It includes the controversial Article 7, a provision that allows French law enforcement and its tech contractors to experiment with intelligent video

surveillance before, during and after the 2024 Olympics, and Article 10, which specifically permits the use of AI software to review video and camera feeds. These laws make France the first EU country to legalize such a wide-reaching AI-powered surveillance system.

Scholars, civil society groups and civil liberty advocates have pointed out that these articles are contrary to the General Data Protection Regulation and the EU's efforts to regulate AI. They argue that Article 7 specifically violates the General Data Protection Regulation's provisions protecting biometric data.

French officials and tech company representatives have said that the AI software can accomplish its goals of identifying and flagging those specific types of events without identifying people or running afoul of the General Data Protection Regulation's restrictions around processing of biometric data. But European civil rights organizations have pointed out that if the purpose and function of the algorithms and AI-driven cameras are to detect specific suspicious events in public spaces, these systems will necessarily "capture and analyse physiological features and behaviours" of people in these spaces. These include body positions, gait, movements, gestures and appearance. The critics argue that this is biometric data being captured and processed, and thus France's law violates the General Data Protection Regulation.

AI-powered security – at a cost

For the French government and the AI companies so far, the AI surveillance has been a mutually beneficial success. The algorithmic watchers are being used more and give governments and their tech collaborators much more data than humans alone could provide.

But these AI-enabled surveillance systems are poorly regulated and subject to little in the way of independent testing. Once the data is collected, the potential for further data analysis and privacy invasions is enormous.

Anne Toomey McKenna, Visiting Professor of Law, *University of Richmond*

P.S.

• The Conversation. Publié: 17 juillet 2024, 14:28 CEST.

This article is republished from The Conversation under a Creative Commons license. Read the original article.

Anne Toomey McKenna, *University of Richmond*

Anne Toomey McKenna (she/her) is a licensed attorney, researcher, and Law Professor working for over two decades at the interdisciplinary intersection of technology, privacy, and law. Professor McKenna is currently a Visiting Law Professor at Richmond Law, where she teaches Evidence, Cyberlaw in Practice (a course she developed), and Information Privacy Law; she has also taught Civil Procedure. She is Affiliated Faculty with Penn State University's Institute for Computational &

Data Sciences and was formerly Penn State Dickinson Law's Distinguished Scholar of Cyber Law & Policy. Professor McKenna is the Co-Chair of the AI Policy Committee for the world's largest technical professional organization, the Institute for Electrical and Electronics Engineers (IEEE), and Co-Chair of IEEE's Privacy, Equity, and Justice in AI Subcommittee.

As part of her work educating, researching, writing, and advising about cutting edge legal and societal issues surrounding privacy, data, technology (including machine learning and artificial intelligence), and surveillance, Professor McKenna collaborates regularly with agency, business, institution, and policy leaders at the highest levels. Professor McKenna brings extensive experiential depth and understanding to her work in these interdisciplinary subjects. That depth and understanding flows from her extensive research, publications, and legal teaching experience combined with her two-plus decades of work as a trial attorney representing clients and handling complex civil litigation in federal and state courts in Maryland and Washington, D.C. That experience includes handling and advising about matters that involve:

• emerging technologies and the law, including artificial intelligence, autonomous systems, and biometric identification systems
• electronic searches and surveillance, electronic evidence
• federal electronic surveillance and hacking laws, including ECPA and CFAA, and state legislation involving data privacy, surveillance, tracking, and evidence
• data practices, data privacy laws, and data breach
• satellite surveillance and data (geodata, geolocation, geofences), and cellular tracking
• online content and speech issues (including Section 230 of the Communications Decency Act,
• mis- and disinformation), website policies, and compliance
• tort and contract-based privacy claims; school and workplace privacy