



**The Journal of Robotics,
Artificial Intelligence & Law**

Editor's Note: AI Developments

Steven A. Meyerowitz

National Security Commission on Artificial Intelligence Final Report Prioritizes U.S. Global Competition, Conflict Preparation, and Enhanced Protection of Privacy and Civil Liberties

Katherine Sheriff and K.C. Halm

Advancing America's Dominance in AI: The 2021 National Defense Authorization Act's AI Developments

Jonathan M. Baker, Adelia R. Cliffe, Kate M. Growley, Laura J. Mitchell Baker, and Michelle D. Coleman

FDA Releases Action Plan for Artificial Intelligence/Machine Learning-Enabled Software as a Medical Device

Nathan A. Brown, Christin Helms Carey, and Emily I. Gerry

Deepfake Litigation Risks: The Collision of AI's Machine Learning and Manipulation

Erin M. Bosman, Christine E. Lyon, Michael Burshteyn, and Benjamin S. Kagel

FBI Warns Companies of "Almost Certain" Threats from Deepfakes

Matthew F. Ferraro, Jason C. Chipman, and Benjamin A. Powell

Prepare for the Impending Wave of Facial Recognition Technology Regulation—Before It's Too Late

David J. Oberly

Considerations in Machine Learning-Led Programmatic Underwriting

Scott T. Lashway, Christopher A. Lisy, and Matthew M.K. Stein

Making Safer Robotic Devices

William D. Kennedy, James D. Burger, and Frank A. Bruno

OFAC Settles With Digital Currency Services Provider for Apparent Violations of Multiple Sanctions Programs

Gustavo J. Membiela and Natalia San Juan

Report on ExamSoft's ExamID Feature (and a Method to Bypass It)

Gabe Teninbaum

Current Developments: AI Research, Crypto Cases Make News

Victoria Prussen Spears

Everything Is Not *Terminator*: The AI Genie Bottle

John Frank Weaver

- 239 Editor’s Note: AI Developments**
Steven A. Meyerowitz
- 243 National Security Commission on Artificial Intelligence Final Report
Prioritizes U.S. Global Competition, Conflict Preparation, and Enhanced
Protection of Privacy and Civil Liberties**
Katherine Sheriff and K.C. Halm
- 251 Advancing America’s Dominance in AI: The 2021 National Defense
Authorization Act’s AI Developments**
Jonathan M. Baker, Adelia R. Cliffe, Kate M. Growley,
Laura J. Mitchell Baker, and Michelle D. Coleman
- 255 FDA Releases Action Plan for Artificial Intelligence/Machine
Learning–Enabled Software as a Medical Device**
Nathan A. Brown, Christin Helms Carey, and Emily I. Gerry
- 261 Deepfake Litigation Risks: The Collision of AI’s Machine Learning and
Manipulation**
Erin M. Bosman, Christine E. Lyon, Michael Burshteyn, and
Benjamin S. Kagel
- 267 FBI Warns Companies of “Almost Certain” Threats from Deepfakes**
Matthew F. Ferraro, Jason C. Chipman, and Benjamin A. Powell
- 271 Prepare for the Impending Wave of Facial Recognition Technology
Regulation—Before It’s Too Late**
David J. Oberly
- 277 Considerations in Machine Learning-Led Programmatic Underwriting**
Scott T. Lashway, Christopher A. Lisy, and Matthew M.K. Stein
- 283 Making Safer Robotic Devices**
William D. Kennedy, James D. Burger, and Frank A. Bruno
- 289 OFAC Settles With Digital Currency Services Provider for Apparent
Violations of Multiple Sanctions Programs**
Gustavo J. Membiela and Natalia San Juan
- 293 Report on ExamSoft’s ExamID Feature (and a Method to Bypass It)**
Gabe Teninbaum
- 301 Current Developments: AI Research, Crypto Cases Make News**
Victoria Prussen Spears
- 311 Everything Is Not *Terminator*: The AI Genie Bottle**
John Frank Weaver

EDITOR-IN-CHIEF

Steven A. Meyerowitz

President, Meyerowitz Communications Inc.

EDITOR

Victoria Prussen Spears

Senior Vice President, Meyerowitz Communications Inc.

BOARD OF EDITORS

Miranda Cole

Partner, Covington & Burling LLP

Kathryn DeBord

Partner & Chief Innovation Officer, Bryan Cave LLP

Melody Drummond Hansen

Partner, O'Melveny & Myers LLP

Paul B. Keller

Partner, Allen & Overy LLP

Garry G. Mathiason

Shareholder, Littler Mendelson P.C.

Elaine D. Solomon

Partner, Blank Rome LLP

Linda J. Thayer

Partner, Finnegan, Henderson, Farabow, Garrett & Dunner LLP

Edward J. Walters

Chief Executive Officer, Fastcase Inc.

John Frank Weaver

Attorney, McLane Middleton, Professional Association

THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW (ISSN 2575-5633 (print) /ISSN 2575-5617 (online) at \$495.00 annually is published six times per year by Full Court Press, a Fastcase, Inc., imprint. Copyright 2021 Fastcase, Inc. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated into any information retrieval system without the written permission of the copyright owner. For customer support, please contact Fastcase, Inc., 711 D St. NW, Suite 200, Washington, D.C. 20004, 202.999.4777 (phone), 202.521.3462 (fax), or email customer service at support@fastcase.com.

Publishing Staff

Publisher: Morgan Morrisette Wright

Journal Designer: Sharon D. Ray

Cover Art Design: Juan Bustamante

Cite this publication as:

The Journal of Robotics, Artificial Intelligence & Law (Fastcase)

This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

Copyright © 2021 Full Court Press, an imprint of Fastcase, Inc.

All Rights Reserved.

A Full Court Press, Fastcase, Inc., Publication

Editorial Office

711 D St. NW, Suite 200, Washington, D.C. 20004

<https://www.fastcase.com/>

POSTMASTER: Send address changes to THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW, 711 D St. NW, Suite 200, Washington, D.C. 20004.

Articles and Submissions

Direct editorial inquiries and send material for publication to:

Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc.,
26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@
meyerowitzcommunications.com, 646.539.8300.

Material for publication is welcomed—articles, decisions, or other items of interest to attorneys and law firms, in-house counsel, corporate compliance officers, government agencies and their counsel, senior business executives, scientists, engineers, and anyone interested in the law governing artificial intelligence and robotics. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the Editorial Content appearing in these volumes or reprint permission, please contact:

Morgan Morrisette Wright, Publisher, Full Court Press at mwright@fastcase.com
or at 202.999.4878

For questions or Sales and Customer Service:

Customer Service

Available 8 a.m.–8 p.m. Eastern Time

866.773.2782 (phone)

support@fastcase.com (email)

Sales

202.999.4777 (phone)

sales@fastcase.com (email)

ISSN 2575-5633 (print)

ISSN 2575-5617 (online)

Everything Is Not *Terminator* The AI Genie Bottle

John Frank Weaver*

Earlier this year, Amnesty International announced its “Ban the Scan” campaign in New York City. It warns that “[f]acial recognition technology can amplify racially discriminatory policing” and that “Black and minority communities are at risk of being misidentified and falsely arrested—in some instances, facial recognition has been 95% inaccurate.”¹ The organization is asking New York residents to contact the New York Police Department and the New York City Council about banning facial recognition technology. Amnesty is also on the steering committee of the Campaign to Stop Killer Robots (“CSKR”), another organization working to eliminate a particular type of artificial intelligence system (“AIS”): fully autonomous weapons.² CSKR is a coalition of non-governmental organizations that seek to retain “meaningful human control over targeting and attack decisions by prohibiting development, production, and use of fully autonomous weapons.”³

It is hard not to admire the principles and goals of Amnesty International and the other organizations behind CSKR. Having concluded that facial recognition technology and fully autonomous weapons are AIS that can result in discriminatory or deadly action, they have put their energy into banning those technologies. It makes a certain amount of sense. Those technologies have readily apparent human costs; the most direct way to prevent those human costs is to eliminate the technologies causing them.

But just because that is the most direct way, it does not mean it is the easiest. Technology is like a genie—sufficiently advanced, it is like magic, but it will not go back in its bottle once released. Much of that can be traced to human beings’ desire to see the potential for good in scientific advances, even if those advances create equal potential for danger and injury. That is as true for AI as any other technology. And in the same way that a genie can be useful if you word your wish carefully, nearly any type of AIS can be useful if governed appropriately.

Asymmetrical Advantages

The problem with banning any technology is that it requires all parties to cease using and developing a line of technology for the ban to be successful. This is extremely unlikely for two reasons. First, there are almost always outliers that refuse to join in such an effort. Second, when the potential benefits of the new technology are substantial, like with many AIS, parties are unlikely to abstain from developing it due to concern that other parties will continue to develop the technology, leaving the abstaining parties at a disadvantage.

The latter scenario creates asymmetrical use of the technology, as one group rejects it due to its dangers while another group uses the technology and benefits from its advantages. This essentially recreates the initial experience of technological change, when only early adopters receive the technology's benefits. As an example, imagine if over the past 20 years traditional retailers refused to develop their e-commerce functionalities after the emergence of the internet. Amazon is the most dominant player in that space now, but without Wal-Mart, Target, etc., also selling goods online, they would have gone out of business or contracted significantly.

The “Ban the Scan” movement and CSKR run into the same problem. By asking parties in New York City—the city government, private landlords, etc.—to prohibit facial recognition software, organizers want them to refuse the benefits of that technology, but that creates asymmetrical use of the AIS. Landlords that adopt the systems are likely to benefit from improved security and cost savings. The concern is even more pronounced in law enforcement circles: if the police decline to use a lawful technology, they know that they give an advantage to criminals that the AIS might otherwise dissuade or identify.

Technology Changes

The asymmetrical dilemma facing nations contemplating the adoption of autonomous weapons systems is stark: do they risk their security by refusing to develop AIS if they believe adversarial nations will continue to develop the technology? The history of banning weapons technologies is spotty at best, a complete failure at worst. Anti-weapons activists frequently point to the success of

the Anti-Personnel Mines Convention⁴ as evidence that organized efforts to prohibit military technologies can be successful. The International Campaign to Ban Landmines (“ICBL”) notes that 80 percent of the world’s nations have joined the treaty, making it one of the most widely accepted treaties.⁵

I admire the organization’s purpose and hope that it reaches its goals of disarming and clearing all mines, while also helping the millions of people who have been injured by the weapons. However, there is evidence indicating that nations began to rely less on landmines because advances in military technology made them less effective. As *The New York Times* reported in 2010, “Some analysts say the rationale [for refusing to sign the Convention] is even weaker now than it was in 1997 [when the Anti-Personnel Mines Convention was first signed]. Technological advances have enabled the Pentagon to create explosives that function like mines but are detonated remotely, making them permissible under the treaty. The United States has not used land mine since 1991,” despite not being a party to the treaty.⁶

That is not to say that ICBL’s efforts have been wasted. The organization has raised awareness of the horrible suffering landmines cause, made nations accountable for their landmine use, and helped victims. The group’s Nobel Peace Prize is well earned. However, I strongly suspect that countries stopped using landmines because their military technology needs changed, not because they felt pressured to stop using them.

What Advocacy Groups Can Do

The ICBL’s achievements, if not outright success, provide a road map for AIS-centric groups like Ban the Scan and CSKR. They might not be able to convince governments to prohibit the technologies, but they can (1) bring attention to the injustices, damages, and deaths produced by the AIS; (2) hold parties accountable; and (3) influence government policies that limit the worst parts of the AIS. Those are useful functions that will make those technologies better.

Ban the Scan and CSKR already populate their websites with statements about the dangers of facial recognition AI and AI weapons. In addition to its statements above about facial recognition software’s inaccuracies and potential to contribute to racial

discrimination, Ban the Scan also represents that facial recognition technology “is developed through scraping millions of images from social media profiles without permission” and has been used 22,000 times in New York City since 2017.⁷

CSKR warns that “[f]ully autonomous weapons would make tragic mistakes with unanticipated consequences” that “could make the decision to go to war easier and shift the burden of conflict even further on to civilians.”⁸ The organization worries this type of AIS would be unable to distinguish civilians from combatants or abide by other core principles of the laws of war.⁹

Some of these representations are overblown. For example, a 2018 study of one-to-one matching AIS (i.e., confirming a photo matches a different photo of the same person in a database) from the National Institute of Standards and Technology reported that just .2 percent of the algorithms failed to perform the task.¹⁰ However, concerns about facial recognition software exacerbating racial bias¹¹ and AI weapon systems failing to properly identify enemy combatants before discharging their weapons¹² are very legitimate concerns that everyone should be worried about, particularly the people responsible for adopting those systems.

Ban the Scan aims to make sure people are worried, calling on its website visitors to take specific actions to force the city’s government to address facial recognition software, including organizing against the technology and submitting comments to the New York City Council, asking it to reject the use of facial recognition software.¹³ The website has a letter-writing portal and links to organizing tools to help interested individuals. CSKR provides similar resources to assist visitors to contact their governments and collaborate with non-governmental organizations, government representatives, experts, and technology companies that are also interested in eliminating autonomous weapons systems.¹⁴ By converting individuals concerned about the AIS to organizers and advocates, Ban the Scan and CSKR apply pressure to governments and decision-making bodies to hold them accountable for their policies and approaches to these technologies.

Finally, those outreach efforts also influence governments and other groups to change how they govern and regulate the AIS. CSKR lists the worldwide government entities that adopt or pursue policies prohibiting autonomous weapons.¹⁵ Ban the Scan notes recent prohibitions adopted in San Francisco, Boston, and Portland, as well as in New York state schools.¹⁶ I question whether

those bans are long-term solutions, as there will be pressure from other constituencies to implement facial recognition technology, particularly as a security measure in schools.

However, it is good public policy to use a formal pause in the adoption of facial recognition technology to permit those cities and schools to implement policies and procedures designed to minimize the harmful impacts of software. Those policies and procedures should include an assessment process to confirm that each facial recognition AIS developer has taken appropriate actions to minimize or eliminate bias from the technology's algorithms.¹⁷

The Genie Is Out, But That's Not Failure

The lesson organizations like Ban the Scan and CSKR should take is not to stop their efforts or even to change their messaging. They believe that the potential dangers of facial recognition technology and autonomous weapons systems outweigh the potential benefits. That is a legitimate position, and they should continue to pursue the prohibitions they seek. However, when they assess their work, I hope they will consider something other than complete bans a success. Once the AI genie is out of the bottle, it is impossible to put it back in until the technology starts to become obsolete. Even though landmines still exist and some nations have not signed the Anti-Personnel Mines Convention, I doubt that ICBL considers its work a failure. The world is safer, and thousands (if not hundreds of thousands) of people are alive and uninjured because of their efforts. Ban the Scan and CSKR should hope for the same level of success. I hope it for them too.

Notes

* John Frank Weaver, a member of McLane Middleton's privacy and data security practice group, is a member of the Board of Editors of *The Journal of Robotics, Artificial Intelligence & Law* and writes its "Everything Is Not Terminator" column. Mr. Weaver, who may be contacted at john.weaver@mclane.com, has a diverse technology practice that focuses on information security, data privacy, and emerging technologies, including artificial intelligence, self-driving vehicles, and drones.

1. Ban the Scan, Amnesty International, *available at* <https://banthescan.amnesty.org/> ("Ban the Scan Homepage").

2. The Steering Committee also includes organizations like Human Rights Watch, Article 36, PAX, and the International Committee for Robot Arms Control.

3. The Problem, Campaign to Stop Killer Robots, *available at* <https://www.stopkillerrobots.org/learn/#problem>.

4. *Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on Their Destruction*, March 1, 1999, 2056 U.N.T.S 241, <http://www.icbl.org/en-gb/the-treaty/treaty-in-detail/treaty-text.aspx>.

5. Join the Treaty, International Campaign to Ban Landmines, *available at* <http://www.icbl.org/en-gb/finish-the-job/join-the-treaty.aspx>.

6. Mark Landler, “White House is Being Pressed to Reverse Course and Join Land Mine Ban,” *New York Times*, May 7, 2010, http://www.nytimes.com/2010/05/08/world/americas/08mine.html?_r=0.

7. Ban the Scan Homepage, *supra* note 1.

8. Learn, Campaign to Stop Killer Robots, *available at* <https://www.stopkillerrobots.org/learn/>.

9. *Id.*

10. “NIST Evaluation Shows Advance in Face Recognition Software’s Capabilities,” National Institute of Standards and Technology (November 20, 2018), *available at* <https://www.nist.gov/news-events/news/2018/11/nist-evaluation-shows-advance-face-recognition-softwares-capabilities>.

11. See “NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software,” National Institute of Standards and Technology (December 19, 2019), *available at* <https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software> (noting that: “For one-to-one matching, the team saw higher rates of false positives for Asian and African American faces relative to images of Caucasians. The differentials often ranged from a factor of 10 to 100 times, depending on the individual algorithm,” and

“For one-to-many matching [i.e., determining whether the person in the photo has any match in a database], the team saw higher rates of false positives for African American females.”).

12. See Christof Heyns, *Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions*, U.N. Document A/HRC/23/47 (April 9, 2013), https://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A-HRC-23-47_en.pdf, at 12-14 (questioning the ability of AI weapons to properly understand international humanitarian law during armed conflict, including knowing “whether someone is wounded and hors de combat, and also whether soldiers are in the process of surrendering”).

13. Ban the Scan Homepage, *supra* note 1.

14. Act, Campaign to Stop Killer Robots, *available at* <https://www.stopkillerrobots.org/act/>.

15. About, Campaign to Stop Killer Robots, *available at* <https://www.stopkillerrobots.org/about/>.

16. Ban the Scan Homepage, *supra* note 1.

17. See John Frank Weaver, “Everything Is Not *Terminator*: Assessment of Artificial Intelligence Systems,” *The Journal of Robotics, Artificial Intelligence & Law* (January-February 2021), 67-75 (describing the material portions of an assessment of AIS).

- 239 Editor’s Note: AI Developments**
Steven A. Meyerowitz
- 243 National Security Commission on Artificial Intelligence Final Report
Prioritizes U.S. Global Competition, Conflict Preparation, and Enhanced
Protection of Privacy and Civil Liberties**
Katherine Sheriff and K.C. Halm
- 251 Advancing America’s Dominance in AI: The 2021 National Defense
Authorization Act’s AI Developments**
Jonathan M. Baker, Adelia R. Cliffe, Kate M. Growley,
Laura J. Mitchell Baker, and Michelle D. Coleman
- 255 FDA Releases Action Plan for Artificial Intelligence/Machine
Learning–Enabled Software as a Medical Device**
Nathan A. Brown, Christin Helms Carey, and Emily I. Gerry
- 261 Deepfake Litigation Risks: The Collision of AI’s Machine Learning and
Manipulation**
Erin M. Bosman, Christine E. Lyon, Michael Burshteyn, and
Benjamin S. Kagel
- 267 FBI Warns Companies of “Almost Certain” Threats from Deepfakes**
Matthew F. Ferraro, Jason C. Chipman, and Benjamin A. Powell
- 271 Prepare for the Impending Wave of Facial Recognition Technology
Regulation—Before It’s Too Late**
David J. Oberly
- 277 Considerations in Machine Learning-Led Programmatic Underwriting**
Scott T. Lashway, Christopher A. Lisy, and Matthew M.K. Stein
- 283 Making Safer Robotic Devices**
William D. Kennedy, James D. Burger, and Frank A. Bruno
- 289 OFAC Settles With Digital Currency Services Provider for Apparent
Violations of Multiple Sanctions Programs**
Gustavo J. Membiela and Natalia San Juan
- 293 Report on ExamSoft’s ExamID Feature (and a Method to Bypass It)**
Gabe Teninbaum
- 301 Current Developments: AI Research, Crypto Cases Make News**
Victoria Prussen Spears
- 311 Everything Is Not *Terminator*: The AI Genie Bottle**
John Frank Weaver

EDITOR-IN-CHIEF

Steven A. Meyerowitz

President, Meyerowitz Communications Inc.

EDITOR

Victoria Prussen Spears

Senior Vice President, Meyerowitz Communications Inc.

BOARD OF EDITORS

Miranda Cole

Partner, Covington & Burling LLP

Kathryn DeBord

Partner & Chief Innovation Officer, Bryan Cave LLP

Melody Drummond Hansen

Partner, O'Melveny & Myers LLP

Paul B. Keller

Partner, Allen & Overy LLP

Garry G. Mathiason

Shareholder, Littler Mendelson P.C.

Elaine D. Solomon

Partner, Blank Rome LLP

Linda J. Thayer

Partner, Finnegan, Henderson, Farabow, Garrett & Dunner LLP

Edward J. Walters

Chief Executive Officer, Fastcase Inc.

John Frank Weaver

Attorney, McLane Middleton, Professional Association

THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW (ISSN 2575-5633 (print) /ISSN 2575-5617 (online) at \$495.00 annually is published six times per year by Full Court Press, a Fastcase, Inc., imprint. Copyright 2021 Fastcase, Inc. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated into any information retrieval system without the written permission of the copyright owner. For customer support, please contact Fastcase, Inc., 711 D St. NW, Suite 200, Washington, D.C. 20004, 202.999.4777 (phone), 202.521.3462 (fax), or email customer service at support@fastcase.com.

Publishing Staff

Publisher: Morgan Morrisette Wright

Journal Designer: Sharon D. Ray

Cover Art Design: Juan Bustamante

Cite this publication as:

The Journal of Robotics, Artificial Intelligence & Law (Fastcase)

This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

Copyright © 2021 Full Court Press, an imprint of Fastcase, Inc.

All Rights Reserved.

A Full Court Press, Fastcase, Inc., Publication

Editorial Office

711 D St. NW, Suite 200, Washington, D.C. 20004

<https://www.fastcase.com/>

POSTMASTER: Send address changes to THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW, 711 D St. NW, Suite 200, Washington, D.C. 20004.

Articles and Submissions

Direct editorial inquiries and send material for publication to:

Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc.,
26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@
meyerowitzcommunications.com, 646.539.8300.

Material for publication is welcomed—articles, decisions, or other items of interest to attorneys and law firms, in-house counsel, corporate compliance officers, government agencies and their counsel, senior business executives, scientists, engineers, and anyone interested in the law governing artificial intelligence and robotics. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the Editorial Content appearing in these volumes or reprint permission, please contact:

Morgan Morrisette Wright, Publisher, Full Court Press at mwright@fastcase.com
or at 202.999.4878

For questions or Sales and Customer Service:

Customer Service

Available 8 a.m.–8 p.m. Eastern Time

866.773.2782 (phone)

support@fastcase.com (email)

Sales

202.999.4777 (phone)

sales@fastcase.com (email)

ISSN 2575-5633 (print)

ISSN 2575-5617 (online)

Everything Is Not *Terminator* The AI Genie Bottle

John Frank Weaver*

Earlier this year, Amnesty International announced its “Ban the Scan” campaign in New York City. It warns that “[f]acial recognition technology can amplify racially discriminatory policing” and that “Black and minority communities are at risk of being misidentified and falsely arrested—in some instances, facial recognition has been 95% inaccurate.”¹ The organization is asking New York residents to contact the New York Police Department and the New York City Council about banning facial recognition technology. Amnesty is also on the steering committee of the Campaign to Stop Killer Robots (“CSKR”), another organization working to eliminate a particular type of artificial intelligence system (“AIS”): fully autonomous weapons.² CSKR is a coalition of non-governmental organizations that seek to retain “meaningful human control over targeting and attack decisions by prohibiting development, production, and use of fully autonomous weapons.”³

It is hard not to admire the principles and goals of Amnesty International and the other organizations behind CSKR. Having concluded that facial recognition technology and fully autonomous weapons are AIS that can result in discriminatory or deadly action, they have put their energy into banning those technologies. It makes a certain amount of sense. Those technologies have readily apparent human costs; the most direct way to prevent those human costs is to eliminate the technologies causing them.

But just because that is the most direct way, it does not mean it is the easiest. Technology is like a genie—sufficiently advanced, it is like magic, but it will not go back in its bottle once released. Much of that can be traced to human beings’ desire to see the potential for good in scientific advances, even if those advances create equal potential for danger and injury. That is as true for AI as any other technology. And in the same way that a genie can be useful if you word your wish carefully, nearly any type of AIS can be useful if governed appropriately.

Asymmetrical Advantages

The problem with banning any technology is that it requires all parties to cease using and developing a line of technology for the ban to be successful. This is extremely unlikely for two reasons. First, there are almost always outliers that refuse to join in such an effort. Second, when the potential benefits of the new technology are substantial, like with many AIS, parties are unlikely to abstain from developing it due to concern that other parties will continue to develop the technology, leaving the abstaining parties at a disadvantage.

The latter scenario creates asymmetrical use of the technology, as one group rejects it due to its dangers while another group uses the technology and benefits from its advantages. This essentially recreates the initial experience of technological change, when only early adopters receive the technology's benefits. As an example, imagine if over the past 20 years traditional retailers refused to develop their e-commerce functionalities after the emergence of the internet. Amazon is the most dominant player in that space now, but without Wal-Mart, Target, etc., also selling goods online, they would have gone out of business or contracted significantly.

The "Ban the Scan" movement and CSKR run into the same problem. By asking parties in New York City—the city government, private landlords, etc.—to prohibit facial recognition software, organizers want them to refuse the benefits of that technology, but that creates asymmetrical use of the AIS. Landlords that adopt the systems are likely to benefit from improved security and cost savings. The concern is even more pronounced in law enforcement circles: if the police decline to use a lawful technology, they know that they give an advantage to criminals that the AIS might otherwise dissuade or identify.

Technology Changes

The asymmetrical dilemma facing nations contemplating the adoption of autonomous weapons systems is stark: do they risk their security by refusing to develop AIS if they believe adversarial nations will continue to develop the technology? The history of banning weapons technologies is spotty at best, a complete failure at worst. Anti-weapons activists frequently point to the success of

the Anti-Personnel Mines Convention⁴ as evidence that organized efforts to prohibit military technologies can be successful. The International Campaign to Ban Landmines (“ICBL”) notes that 80 percent of the world’s nations have joined the treaty, making it one of the most widely accepted treaties.⁵

I admire the organization’s purpose and hope that it reaches its goals of disarming and clearing all mines, while also helping the millions of people who have been injured by the weapons. However, there is evidence indicating that nations began to rely less on landmines because advances in military technology made them less effective. As *The New York Times* reported in 2010, “Some analysts say the rationale [for refusing to sign the Convention] is even weaker now than it was in 1997 [when the Anti-Personnel Mines Convention was first signed]. Technological advances have enabled the Pentagon to create explosives that function like mines but are detonated remotely, making them permissible under the treaty. The United States has not used land mine since 1991,” despite not being a party to the treaty.⁶

That is not to say that ICBL’s efforts have been wasted. The organization has raised awareness of the horrible suffering landmines cause, made nations accountable for their landmine use, and helped victims. The group’s Nobel Peace Prize is well earned. However, I strongly suspect that countries stopped using landmines because their military technology needs changed, not because they felt pressured to stop using them.

What Advocacy Groups Can Do

The ICBL’s achievements, if not outright success, provide a road map for AIS-centric groups like Ban the Scan and CSKR. They might not be able to convince governments to prohibit the technologies, but they can (1) bring attention to the injustices, damages, and deaths produced by the AIS; (2) hold parties accountable; and (3) influence government policies that limit the worst parts of the AIS. Those are useful functions that will make those technologies better.

Ban the Scan and CSKR already populate their websites with statements about the dangers of facial recognition AI and AI weapons. In addition to its statements above about facial recognition software’s inaccuracies and potential to contribute to racial

discrimination, Ban the Scan also represents that facial recognition technology “is developed through scraping millions of images from social media profiles without permission” and has been used 22,000 times in New York City since 2017.⁷

CSKR warns that “[f]ully autonomous weapons would make tragic mistakes with unanticipated consequences” that “could make the decision to go to war easier and shift the burden of conflict even further on to civilians.”⁸ The organization worries this type of AIS would be unable to distinguish civilians from combatants or abide by other core principles of the laws of war.⁹

Some of these representations are overblown. For example, a 2018 study of one-to-one matching AIS (i.e., confirming a photo matches a different photo of the same person in a database) from the National Institute of Standards and Technology reported that just .2 percent of the algorithms failed to perform the task.¹⁰ However, concerns about facial recognition software exacerbating racial bias¹¹ and AI weapon systems failing to properly identify enemy combatants before discharging their weapons¹² are very legitimate concerns that everyone should be worried about, particularly the people responsible for adopting those systems.

Ban the Scan aims to make sure people are worried, calling on its website visitors to take specific actions to force the city’s government to address facial recognition software, including organizing against the technology and submitting comments to the New York City Council, asking it to reject the use of facial recognition software.¹³ The website has a letter-writing portal and links to organizing tools to help interested individuals. CSKR provides similar resources to assist visitors to contact their governments and collaborate with non-governmental organizations, government representatives, experts, and technology companies that are also interested in eliminating autonomous weapons systems.¹⁴ By converting individuals concerned about the AIS to organizers and advocates, Ban the Scan and CSKR apply pressure to governments and decision-making bodies to hold them accountable for their policies and approaches to these technologies.

Finally, those outreach efforts also influence governments and other groups to change how they govern and regulate the AIS. CSKR lists the worldwide government entities that adopt or pursue policies prohibiting autonomous weapons.¹⁵ Ban the Scan notes recent prohibitions adopted in San Francisco, Boston, and Portland, as well as in New York state schools.¹⁶ I question whether

those bans are long-term solutions, as there will be pressure from other constituencies to implement facial recognition technology, particularly as a security measure in schools.

However, it is good public policy to use a formal pause in the adoption of facial recognition technology to permit those cities and schools to implement policies and procedures designed to minimize the harmful impacts of software. Those policies and procedures should include an assessment process to confirm that each facial recognition AIS developer has taken appropriate actions to minimize or eliminate bias from the technology's algorithms.¹⁷

The Genie Is Out, But That's Not Failure

The lesson organizations like Ban the Scan and CSKR should take is not to stop their efforts or even to change their messaging. They believe that the potential dangers of facial recognition technology and autonomous weapons systems outweigh the potential benefits. That is a legitimate position, and they should continue to pursue the prohibitions they seek. However, when they assess their work, I hope they will consider something other than complete bans a success. Once the AI genie is out of the bottle, it is impossible to put it back in until the technology starts to become obsolete. Even though landmines still exist and some nations have not signed the Anti-Personnel Mines Convention, I doubt that ICBL considers its work a failure. The world is safer, and thousands (if not hundreds of thousands) of people are alive and uninjured because of their efforts. Ban the Scan and CSKR should hope for the same level of success. I hope it for them too.

Notes

* John Frank Weaver, a member of McLane Middleton's privacy and data security practice group, is a member of the Board of Editors of *The Journal of Robotics, Artificial Intelligence & Law* and writes its "Everything Is Not Terminator" column. Mr. Weaver, who may be contacted at john.weaver@mclane.com, has a diverse technology practice that focuses on information security, data privacy, and emerging technologies, including artificial intelligence, self-driving vehicles, and drones.

1. Ban the Scan, Amnesty International, *available at* <https://banthescan.amnesty.org/> ("Ban the Scan Homepage").

2. The Steering Committee also includes organizations like Human Rights Watch, Article 36, PAX, and the International Committee for Robot Arms Control.

3. The Problem, Campaign to Stop Killer Robots, *available at* <https://www.stopkillerrobots.org/learn/#problem>.

4. *Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on Their Destruction*, March 1, 1999, 2056 U.N.T.S 241, <http://www.icbl.org/en-gb/the-treaty/treaty-in-detail/treaty-text.aspx>.

5. Join the Treaty, International Campaign to Ban Landmines, *available at* <http://www.icbl.org/en-gb/finish-the-job/join-the-treaty.aspx>.

6. Mark Landler, “White House is Being Pressed to Reverse Course and Join Land Mine Ban,” *New York Times*, May 7, 2010, http://www.nytimes.com/2010/05/08/world/americas/08mine.html?_r=0.

7. Ban the Scan Homepage, *supra* note 1.

8. Learn, Campaign to Stop Killer Robots, *available at* <https://www.stopkillerrobots.org/learn/>.

9. *Id.*

10. “NIST Evaluation Shows Advance in Face Recognition Software’s Capabilities,” National Institute of Standards and Technology (November 20, 2018), *available at* <https://www.nist.gov/news-events/news/2018/11/nist-evaluation-shows-advance-face-recognition-softwares-capabilities>.

11. See “NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software,” National Institute of Standards and Technology (December 19, 2019), *available at* <https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software> (noting that: “For one-to-one matching, the team saw higher rates of false positives for Asian and African American faces relative to images of Caucasians. The differentials often ranged from a factor of 10 to 100 times, depending on the individual algorithm,” and

“For one-to-many matching [i.e., determining whether the person in the photo has any match in a database], the team saw higher rates of false positives for African American females.”).

12. See Christof Heyns, *Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions*, U.N. Document A/HRC/23/47 (April 9, 2013), https://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A-HRC-23-47_en.pdf, at 12-14 (questioning the ability of AI weapons to properly understand international humanitarian law during armed conflict, including knowing “whether someone is wounded and hors de combat, and also whether soldiers are in the process of surrendering”).

13. Ban the Scan Homepage, *supra* note 1.

14. Act, Campaign to Stop Killer Robots, *available at* <https://www.stopkillerrobots.org/act/>.

15. About, Campaign to Stop Killer Robots, *available at* <https://www.stopkillerrobots.org/about/>.

16. Ban the Scan Homepage, *supra* note 1.

17. See John Frank Weaver, “Everything Is Not *Terminator*: Assessment of Artificial Intelligence Systems,” *The Journal of Robotics, Artificial Intelligence & Law* (January-February 2021), 67-75 (describing the material portions of an assessment of AIS).

