ALSO IN THIS ISSUE

n addition to this special issue on "Trustworthy Al-Part III," I'd like to add three articles from our queue of regular articles. I thank the authors for their patience in waiting for their accepted articles to be published. *Computer* has seen an uptick in the number of submissions, and we have a backlog of accepted articles.

The authors of the first article^{A1} discuss the concept of zero-touch networks. Zero-touch networks are designed for intelligent resource provisioning strategies, where multiple service providers collaboratively offer computational and storage resources. This article discusses combining distributed AI with zero-touch provisioning for edge networks. The authors argue that this combination should help to manage network devices intelligently and minimize human intervention.

The authors of the second article A2 discuss the potential of machine learning models leaking private information. This possibility has inspired legislative enforcement of the idea that people have a "right to be forgotten." The article explains that to "be forgotten," machine unlearning methods have been proposed for erasing the contributions of data on training models. This review of machine unlearning techniques includes exact and approximate unlearning methods, verification mechanisms, and potential attacks.

Digital Object Identifier 10.1109/MC.2024.3352352 Date of current version: 1 March 2024 The authors of the third article A3 survey the history of computer vision in video surveillance, from early approaches for people detection and tracking to action analysis and language description. The article focuses on privacy concerns, and it suggests that the relationship between video surveillance and privacy is a paradox since surveillance increases safety but does not always require people identification. Through experiments, the authors highlight that the paradox of surveillance and privacy can be solved using AI.

-Jeffrey Voas[®], Editor in Chief

APPENDIX: RELATED ARTICLES

- A1. A. Hazra et al., "Distributed AI in zero-touch provisioning for edge networks: Challenges and research directions," Computer, vol. 57, no. 3, pp. 69–78, Mar. 2024, doi: 10.1109/MC.2023.3334913.
- A2. Y. Qu, X. Yuan, M. Ding, W. Ni, T. Rakotoarivelo, and D. Smith, "Learn to unlearn: Insights into machine unlearning," *Computer*, vol. 57, no. 3, pp. 79–90, Mar. 2024, doi: 10.1109/MC.2023. 3333319.
- A3. R. Cucchiara, L. Baraldi, M. Cornia, and S. Sarto, "Video surveillance and privacy: A solvable paradox?" Computer, vol. 57, no. 3, pp. 91–100, Mar. 2024, doi: 10.1109/MC.2023.3316696.

becomes, the more "believers" that will be generated. (Viral information quickly fosters new affinity groups of like-minded individuals.)

disinformation because of its potential to spark violence. Note that not all incorrect information is human generated. Artificial intelligence (AI)

A key problem with any form of information dissemination is the adage that "you can't put toothpaste back into the tube."

Governments are aware that social media is an inexpensive tool for adversaries to engage in information warfare campaigns to sow public distrust. Governments also monitor extreme right-wing and left-wing can create fake information, including deepfakes. Because of automation, AI-generated fake information can be created as quickly as it can go viral. In "Report: Obama Advised Biden on AI Strategy," the article states:

"According to NBC, the White House is particularly concerned about the role AI could play in spreading misinformation about elections." And there is evidence that creating fake news creates jobs in some nations while not breaking any laws in those countries. 4

Note also that not all of us are equally vulnerable to incorrect information. Devout skeptics are probably the wariest, and the elderly are the more susceptible; the elderly are particularly vulnerable to *phishing* attacks. (Phishing attacks can be thought of as a form of deceptive disinformation.) Children are also vulnerable. Let's not overlook the growing concern that social media may be ruining