AI AND SPYING

BRUCE SCHNEIER[†]

Spying and surveillance are related, but they're different. If I hired a private detective to spy on you, that detective could hide a bug in your home or car, tap your phone, and listen to everything you said.[1] At the end, I would get a report of the conversations you had and the contents of those conversations.[2] If I hired that same private detective to put you under surveillance, I would get a different report: where you went, who you talked to, what you purchased, what you did.[3]

Before the Internet, putting someone under surveillance was both expensive and time-consuming. You had to manually follow someone around, noting where they went, what they purchased, who they talked to, what they did, and what they read. That world is forever gone. Our phones track our locations.[4] Credit cards track our purchases.[5] Email providers, messaging services, and social media apps track who we talk to, and e-readers know what we read.[6] Computers collect data about what you're doing on them.[7]

As both storage and processing have become cheaper, all of this data is increasingly saved

[†] Bruce Schneier is an internationally renowned security technologist, called a "security guru" by the Economist. He is the New York Times best-selling author of 14 books—including Rewiring Democracy and A Hacker's Mind—as well as hundreds of articles, essays, and academic papers. His long-running newsletter and blog, "Schneier on Security," is one of the most popular sources of cybersecurity news on the internet. Schneier is a Fellow and Lecturer in Public Policy at the Harvard Kennedy School and the Munk School at the University of Toronto. He is a fellow at the Berkman-Klein Center for Internet and Society at Harvard University, a board member of the Electronic Frontier Foundation and AccessNow, and an advisory board member of EPIC and VerifiedVoting.org. He is also the Chief of Security Architecture at Inrupt, Inc.

[1] *See, e.g.,* Forrest Plesko, *On the Ethical use of Private Investigators*, 92 DENV. L. REV. F. 157 (May 7, 2015); *Forensic Examination of Digital Devices in Civil Litigation: The Legal, Ethical, and Technical Traps*, 24 PROF. LAW. 1 (Mar. 1, 2016), https://www.americanbar.org/groups/professional_responsibility/publications/professional_lawyer/2016/volume-24-number-1/forensic_examination_digital_devices_civil_litigation_legal_ethical_and_technical_traps; Investigations America, *Investigators Can Help Find Bugs, Listening Devices, and Hidden Camera* (Nov. 19, 2024), https://investigationsamerica.com/investigators-can-help-find-bugs-listening-devices-and-hidden-cameras [https://perma.cc/DTH8-EFQ2].

[2] *See* Plesko, *supra* Note 1.

[3] *Id.*

[4] Jennifer Valentino-DeVries, *How Your Phone Is Used to Track You, and What You Can Do About It*, N.Y. TIMES (Aug. 19, 2020), https://www.nytimes.com/2020/08/19/technology/smartphone-location-tracking-opt-out.html [https://perma.cc/C2ZN-J5KW].

[5] Emily Steel, *Mastercard Pitches Holiday Spending Data to Marketers*, CNBC (Oct. 17, 2012), https://www.cnbc.com/2012/10/17/mastercard-pitches-holiday-spending-data-to-marketers.html [https://perma.cc/FM5R-U32K].

[6] Yael Grauer, *Why Email Providers Scan Your Emails*, CONSUMER REPORTS (July 2, 2021), https://www.consumerreports.org/electronics/privacy/why-email-providers-scan-your-emails-a8433077582/ [https://perma.cc/ 9V88-UF6K].

[7] Gregg Keizer, *EFF condemns Windows 10 data collection*, COMPUTERWORLD (Aug. 22, 2016), https://www.computerworld.com/article/1676831/eff-condemns-windows-10-data-collection-2.html [https://perma.cc/554P-6WRZ].

and used.[8] What was once manual and individual has become bulk and mass. Surveillance is the business model of the Internet, and there's no reasonable way for us to opt out of it.[9]

Spying is another matter. The technologies of wiretapping and room bugs are not new, but processing output from these technologies still takes work and requires someone to listen to and make sense of the conversations. Yes, laws like CALEA make it easier for the police to spy on phone conversations,[10] and spyware companies like NSO Group help governments hack into people's smartphones,[11] but someone still must listen to and sort through all the conversations. Governments like China's can censor social media posts based on particular words or phrases, but that is coarse and easy to bypass.[12] Mass spying has always been limited by the need for human labor.[13]

AI is about to change that. Summarization is something modern generative AI systems do well.[14] Give an AI an hour-long meeting, and it will return a one-page summary of what was said.[15] Ask it to search through millions of conversations and organize them by topic, and it'll do that.[16] Want to know who is talking about what? It'll tell you.[17]

[8] Abu Bakar Munir, Siti Hajar Mohd Yasin & Firdaus Muhammad-Sukki, *Big Data: Big Challenges to Privacy and Data Protection*, APPDI (Aug. 19, 2020), https://appdi.org/big-data-big-challenges-to-privacy-and-data-protection/ [https://perma.cc/9JZV-34AS].

[9] *See* Fahmida Y. Rashid, *Surveillance is the Business Model of the Internet: Bruce Schneier*, SCHNEIER ON SEC. (Apr. 9, 2014), https://www.schneier.com/news/archives/2014/04/surveillance_is_the.html [https://perma.cc/EX3L-ZUUH].

[10] *See* Sam Thielman, *Surveillance reform explainer: can the FBI still listen to my phone calls?,* THE GUARDIAN (June. 3, 2025), https://www.theguardian.com/world/2015/jun/03/surveillance-reform-freedom-act-explainer-fbi-phone-calls-privacy [https://perma.cc/32JZ-DF32].

[11] *See* Mark Mazzetti & Ronen Bergman, *A Front Company and a Fake Identity: How the U.S. Came to Use Spyware It Was Trying to Kill.*, N.Y. TIMES (Apr. 2, 2023), https://www.nytimes.com/2023/04/02/us/politics/nso-contract-us-spy.html.

[12] *See* Thorin Klosowski, *Here's What You're Actually Agreeing To When You Accept a Privacy Policy*, N.Y. TIMES: WIRECUTTER (Apr. 14, 2023), https://www.nytimes.com/wirecutter/blog/what-are-privacy-policies/ (noting that privacy policy notices outline a company's data collection practices, but "there's nothing about them that promises any privacy").

[13] *See* Gregory Brazeal, *Mass Seizure and Mass Search*, 22 U. PA. J. OF CONST. L., 1001, 1009 (2020) (discussing that the high cost of human labor as a factor that historically limited the state's ability to surveil the public).

[14] *See* Yang Zhang et al., *A Comprehensive Survey on Automatic Text Summarization with Exploration of LLM-Based Methods*, ARXIV (Mar. 20, 2025), https://arxiv.org/html/2403.02901v2 (stating that AI systems are capable of summarizing large amounts of text, and are improving in their capabilities); Kristian Hammond, *The AI Summarization Dilemma: When Good Enough Isn't Enough,* CTR. FOR ADVANCING SAFETY OF MACH. INTEL. (Aug. 27, 2024), https://casmi.northwestern.edu/news/articles/2024/the-ai-summarization-dilemma-when-good-enough-isnt-enough.html [https://perma.cc/N93L-95S9] (arguing that AI summarization tools are powerful tools in managing information overload).

[15] *See, e.g.*, OTTER AI, https://otter.ai/ [https://perma.cc/L3JS-YSMM] (last visited Dec. 1, 2025) (advertising that its system can "turn conversations into summaries").

[16] *See, e.g.*, Matt Renner & Matt A.V. Chaban, *1,001 real-world gen AI use cases from the world's leading organizations,* GOOGLE CLOUD BLOG (Oct. 9, 2025), https://cloud.google.com/transform/101-real-world-generative-ai-use-cases-from-industry-leaders [https://perma.cc/74ZS-XFC2] (discussing Gemini AI software use by a car company that feeds conversations between passengers to the software, which categorizes the conversations by content and generates alerts to anticipate risky situations); Yicheng Zou et al., *Unsupervised Summarization for Chat Logs with Topic-Oriented Ranking and Context-Aware Auto-Encoders*, ARXIV (June 25, 2021), https://arxiv.org/abs/2012.07300 (discussing that unsupervised AI models can summarize conversations and sort them into categories without human labelling).

[17] *See What is conversational analytics?*, IBM, https://www.ibm.com/think/topics/conversational-analytics [https://perma.cc/SF3W-JHQG] (last visited Dec. 5, 2025).

The technologies aren't perfect by any means, and some of them are still pretty primitive.[18] They sometimes miss things that are important and get things wrong.[19] But so do humans.[20] And, unlike humans, AIs are improving at astonishing rates.[21] They'll get better next year, and even better the year after that.[22] And, more importantly and unlike humans, AI tools can be replicated by the millions.[23] We are about to enter the era of mass spying.[24]

Technological advancements that allowed for mass surveillance fundamentally changed the nature of surveillance.[25] Because the data can all be saved, you can conduct surveillance backwards in time. You can conduct surveillance without even knowing who specifically you want to target.[26] Tell me where this person was last year. List all the red sedans that drove down this road in the past month. List all of the people who purchased all the ingredients for a pressure cooker bomb in the past year. Look for people whose cell phone location puts them close to a specific cell phone more often than usual (a sign of a tail). Find me all the pairs of phones that were moving towards each other, turned themselves off, and then turned themselves on again an hour later while moving away from each other (a sign of a secret meeting).

Just as it changed the nature of surveillance, rapid advancement in technology will change the nature of spying.[27] By automating tasks that used to require human analysis, AI will make vast troves of previously unprocessable data searchable and understandable in bulk and backwards in time.[28] Tell me who has talked about a particular topic in the past month, and how discussions about that topic have evolved. Person A did something; check if someone told them to do it. Find everyone who is plotting a crime, or who is spreading a rumor, or planning to attend a political protest.

There's so much more. To uncover an organizational structure, look for someone who gives

[18] *See* Neil Sahota, *Perfectly Imperfect: Coping With The 'Flaws' Of Artificial Intelligence (AI)*, FORBES (June 15, 2020), https://www.forbes.com/sites/cognitiveworld/2020/06/15/perfectly-imperfect-coping-with-the-flaws-of-artificial-intelligence-ai/ [https://perma.cc/BJC7-MM36].

[19] *See id.*

[20] *See id.*

[21] *See* Ellen Chang, *How fast are AI companies evolving? Check this out.*, HARV. BUS. SCH. (May 12, 2025), https://www.hbs.edu/bigs/perplexity-aravind-srinivas [https://perma.cc/SM8J-2KF8].

[22] *See id.*

[23] Xudong Pan et al., *Frontier AI Systems Have Surpassed the Self-Replicating Red Line* 8–9, ARXIV (Dec. 9, 2024), https://arxiv.org/abs/2412.12140.

[24] Maurizio Guerrero, *The Growing Surveillance State in the US is Far Worse Than You Imagined*, PRISM (July 10, 2025), https://prismreports.org/2025/07/10/surveillance-state-in-u-s-is-far-worse-than-you-imagined.

[25] Catarina Fontes et al., *AI-Powered Public Suveilllance Systems: Why We (Might) Need Them and How We Want Them*, 71 TECH. IN SOC'Y 2 (2022) (discussing the increase in amount of available data and public and private entities using such data for surveillance).

[26] *See* Sarah Taitz, *Five Things to Know About NSA Mass Surveillance and the Coming Fight in Congress*, ACLU (Apr. 11, 2023), https://www.aclu.org/news/national-security/five-things-to-know-about-nsa-mass-surveillance-and-the-coming-fight-in-congress.

[27] Darryl M. West, H*ow AI can enable public surveillance*, BROOKINGS INST. (Apr. 15, 2025), https://www.brookings.edu/articles/how-ai-can-enable-public-surveillance/ (explaining how AI is used for surveillance by both foreign entities and domestic law enforcement).

[28] *Id.* ("Due to its scalability and capacity to examine large data sets, [AI] can study people's behavior and act on that information").

similar instructions to a group of people, then find all the people they have relayed those instructions to. To find people's confidants, look at who they tell secrets to. You can track friendships and alliances as they form and break, in minute detail. In short, you can know everything about what everybody is talking about. I'm sure there are possibilities I can't even imagine.

This mass spying is not limited to conversations on our phones or computers. Just as cameras everywhere fueled mass surveillance, microphones everywhere will fuel mass spying.[29] Siri and Alexa and Google Home are already always listening; the conversations just aren't being saved yet.[30]

Knowing that they are under constant surveillance changes how people behave.[31] They conform and self-censor.[32] Surveillance facilitates social control, and spying will only make this worse.[33]

Corporations will spy on people.[34] Mass surveillance ushered in the era of personalized advertisements.[35] Mass spying will supercharge that industry. Information about what people are talking about, their moods, their secrets[36]—it's all catnip for marketers looking for an edge. The tech monopolies that are currently keeping us all under constant surveillance[37] won't be able to resist collecting and using all of that data.

In the early days of Gmail, Google talked about using people's Gmail content to serve them personalized ads.[38] They stopped doing it, almost certainly because the keyword data they

[29] Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1936 (2013).

[30] Rich Demuro, *How to Stop Your Smart Devices From Eavesdropping*, RICH ON TECH (Jan. 4, 2025), https://richontech.tv/p/how-stop-your-smart-devices-from [https://perma.cc/K5BV-7F4Z].

[31] *How surveillance technology is changing our behavior and our brains*, UTS ONLINE (Jan. 25, 2025), https://studyonline.uts.edu.au/blog/how-surveillance-technology-changing-our-behaviour-and-our-brains [https://perma.cc/V4DA-U7Q3].

[32] *See id.*

[33] Bruce Schneier, *The Internet Enabled Mass Surveillance. A.I. Will Enable Mass Spying.*, SLATE (Dec. 4, 2023), https://slate.com/technology/2023/12/ai-mass-spying-internet-surveillance.html [https://perma.cc/2Y9M-YMUD].

[34] *Id.*

[35] *Id.*

[36] Valentin Saitarli, *Emotion: The Super Weapon of Marketing and Advertising*, FORBES, (Apr. 14, 2022), https://www.forbes.com/councils/forbesagencycouncil/2019/11/04/emotion-the-super-weapon-of-marketing-and-advertising/ [https://perma.cc/HRN2-NYY5].

[37] *FTC Staff Report Finds Large Social Media and Video Streaming Companies Have Engaged in Vast Surveillance of Users with Lax Privacy Controls and Inadequate Safeguards for Kids and Teens*, FED. TRADE COMM'N, (Sep. 19, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-staff-report-finds-large-social-media-video-streaming-companies-have-engaged-vast-surveillance [https://perma.cc/9PGC-MG8Q].

[38] Rosa Golijan, *Gmail will soon personalize ads based on your emails*, NBC NEWS, (Mar. 30, 2011), https://www.nbcnews.com/tech/tech-news/gmail-will-soon-personalize-ads-based-your-emails-flna124201 [https://perma.cc/9TVM-H3WN].

collected was so poor—and therefore not useful for marketing purposes.[39] That will soon change. Maybe Google won't be the first to spy on their users' conversations, but once others start, they won't be able to resist. Their true customers—advertisers[40]—will demand it.

Governments will use these capabilities as well. Many countries around the world already use mass surveillance.[41] In the future they will also engage in mass spying. We could limit this capability. We could prohibit mass spying. We could pass strong data privacy rules.[42] But we haven't done anything to limit mass surveillance.[43] Why would spying be any different?

[39] Laurel Wamsley, *Google Says It Will No Longer Read Users' Emails to Sell Targeted Ads*, NPR, (June 26, 2017), https://www.npr.org/sections/thetwo-way/2017/06/26/534451513/google-says-it-will-no-longer-read-users-emails-to-sell-targeted-ads [https://perma.cc/S6D6-7Z8F].

[40] *How our business works*, GOOGLE, https://about.google/company-info/how-our-business-works [https://perma.cc/U9JS-UHR9].

[41] Steve Feldstein, *The Global Expansion of AI Surveillance*, CARNEGIE ENDOWMENT FOR INT'L PEACE (Sep. 17, 2019), https://carnegieendowment.org/research/2019/09/the-global-expansion-of-ai-surveillance [https://perma.cc/ARG3-6DMD].

[42] For example, the European Union passed the General Data Protection Regulation (GDPR) in 2016, which protects data privacy and the right to data portability. Council Regulation 2016/679, art. 1, 2016 O.J. (L 119) 1.

[43] *See Report: State Laws are Failing to Protect Privacy*, ELEC. PRIV. INFO. CTR. (Feb. 1, 2024), https://epic.org/release-report-state-laws-are-failing-to-protect-privacy/ (describing Congress's failure to pass comprehensive data privacy laws and the inadequacy of state privacy laws).