TRYING FOR THE TRIFECTA

TELEHEALTH MEETS AI MEETS CYBERSECURITY

By Thomas P. Keenan

The social disruption of the COVID-19 pandemic has accelerated two powerful trends in health care—telemedicine (TM) and artificial intelligence/machine learning (AI/ML). Advocates of digital transformation let out of collective "Yes!" as long-awaited changes happened almost overnight in early 2020. Then, the ants of cybersecurity came along to spoil the picnic!

First, the good news.

- Suddenly, it became acceptable to "see" your doctor electronically; you could even send a picture of that wart on your foot, though perhaps not that rash in your groin.[1] Health insurers, including Medicare, that had frowned upon telemedicine suddenly decided it was a great idea.
- The success of countries like South Korea in "stopping the virus in its tracks"[2] demonstrated that a technology-based, data-driven approach to a major health problem could actually work. It also raised troubling issues of privacy as some countries enforced quarantine with mandatory smartphone apps, license plate readers, even tracking of people through cell phone pings and credit card transactions.

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

High hopes for AI in medicine go back decades. In the 1980s I interviewed one of the early adopters of PUFF, an expert system for the diagnosis of lung disease.[3] I asked this doctor if PUFF was any good. "It's a better diagnostician than I am," he laughed. The doctor further explained that, when given a stack of patient files and chest X-rays, after about five or six he's getting tired, and after ten he's "ready to go the bar." By contrast, the machine treats each case with unbiased, fresh eyes, giving consistent results. "It [PUFF] also knows things I haven't a clue about," he added. One of the many experts who contributed knowledge to PUFF was a tropical medicine specialist. This contribution enabled the system to spot a rare lung problem caused by breathing bat guano in Central American caves.

PUFF was an example of a rule-based expert system. It sifted through carefully formatted symptoms and lab results, then spewed out a result like "THE LOW DIFFUSING CAPACITY, IN COMBINATION WITH OBSTRUCTION AND A HIGH TOTAL LUNG CAPACITY IS CONSISTENT WITH A DIAGNOSIS OF EMPHYSEMA."[4] Impressive for its time, but PUFF would feel like a dummy (if programs could feel—a fascinating legal question[5]) beside one of today's $40 smart speakers.

Expert systems like PUFF had their day, but real progress in AI required two more things: massive computing power and new approaches.

We got the first, in 1997, when IBM's Deep Blue program stunned the world by defeating human chess champion Garry Kasparov. It used specialized hardware and a brute force approach that could evaluate 200 million chess positions per second, applying rules like working out the value of having your king in a safe position.

Of even greater relevance is the 2011 victory of the same company's Watson over human *Jeopardy!* champs Brad Rutter and Ken Jennings. According to AI expert Murray Campbell, that system "used a machine-learning-based system that took a lot of data that existed in the world—things like Wikipedia and so on—and used that data to learn how to answer questions about the real world."[6]

Today, we think nothing of saying, "Hey Google, turn off all the lights" or "Alexa, tell me a joke about rabbits," confident that our AI-enabled speakers will understand and obey us. Because their knowledge base and ML functionality reside in a remote computer, our virtual assistants will keep getting smarter and better informed. Perhaps Alexa will have a joke about "one-legged rabbits" the next time I ask "her."[7]

AI is already embedded in many aspects of today's medicine, including surgery. According to trade publication *Robotics Online*, "AI can determine patterns within surgical procedures to improve best practices and to improve a surgical robots' control accuracy to submillimeter precision."[8]

How about chest X-rays? In the almost forty years since PUFF premiered, have we figured out how to automate that? The answer is a qualified yes. In a study published in 2019,[9] Giovanni Montana and colleagues used 470,388 adult chest X-rays that had been analyzed by human radiologists to train a neural network. They then gave the system an independent set of 15,887 X-rays to review. The program called true positives "positive" seventy-three percent of the time and identified true negatives ninety-four percent of the time. While that isn't perfect, it could certainly help to unclog the X-ray reading backlogs. The authors conclude that "we have demonstrated the feasibility of AI for triaging chest radiographs."[10]

One of the problems with AI in medicine is that it can be *too* observant, finding patterns that are not clinically meaningful. Speaking to *Science*, neurosurgeon Eric Oermann noted that many of his hospital's

sickest patients had their X-rays done with portable machines. The hospital's AI algorithm started to incorrectly associate the mere use of a portable unit with greater illness.[11]

No technology is perfect. Even Amazon's Alexa, which has been trained on billions of interactions with millions of voices, can spew out some honkers. In a YouTube video, an innocent toddler asks Alexa to "Play Twinkle Twinkle." The system hears this as "pussyanaldildo" and begins to reply to *that* query, to the horrified shouts of the adults in the room.[12]

Perhaps it was no accident. Alexa uses past interactions and machine learning to tailor her responses to individual user preferences. One commentator on that video made this terse observation—"Dad's browser history!"

TELEHEALTH AND TELEMEDICINE

Canada, where I live, has a long history of using communications technology for healthcare delivery. This is largely driven by geography, given the size of the country. It makes little economic sense to fly a patient 1,000 km each way from Churchill to Winnipeg, Manitoba, to have a toenail fungus checked. Also, Canada's single-payer healthcare system makes the decision to use technology much simpler than in a world with HMOs and insurance companies and private and public providers.

In our most populous province, the Ontario Telemedicine Network (OTN, now part of Ontario Health) reported over 1,000,000 eVisits in 2018–19, serving almost 300,000 patients.[13] In some cases, the link was from a local healthcare facility, often with a nurse alongside the patient. Other eVisits were done from the patient's home computer or smartphone. OTN even tested a Virtual Palliative Care program that served 118 patients and garnered an eighty-seven percent positive approval rating from them.[14]

There are some fascinating consequences of telemedicine. One is the generation of precise information about healthcare delivery. There are jurisdictions in Canada (e.g., Alberta) where doctors are paid more for "complex" patient consultations. This is typically determined by the appointment lasting over fifteen minutes. There was some suggestion that doctors were being sloppy in tracking this, or even trying to "game" the system. With telemedicine, data are collected automatically and accurately.

TM can also make services available to a wider population than traditional delivery models. In the U.S., Congresswoman Robin Kelly (D-Illinois) has introduced a bill in the House of Representatives to study the effects on the sudden move to doctors at a distance. She believes that technology can act as an "equalizer" in healthcare delivery.[15]

It can also be a great compromiser of personal privacy.

When COVID-19 struck, Zoom rapidly became the most popular of the videoconference platforms and was adopted by schools, businesses, and, of course, healthcare providers. Part of its appeal was simplicity. You could just send someone a link and they were in your video meeting. You didn't even need to bother with a pesky password.

This quickly led to "Zoombombing," where uninvited guests dropped into video sessions, disrupting them with their comments or, often, their nudity. In addition, Zoom's naming convention for stored recordings was easy to guess. The *Washington Post* reported "Thousands of Zoom Video Calls Left Exposed on Open Web," and said these included therapy sessions, conversations with children, even an explicit demonstration of how to do a Brazilian wax job.[16]

Simon Woodside, co-founder of MedStack, has advised healthcare providers against using Zoom for patient visits.[17] He says the company misstated its use of encryption and "has broken trust." He also points to a Citizen Lab report[18] showing information was routed through servers in China—a potential threat to data sovereignty and user privacy.

HEALTH DATA: PRIVACY AND POTENTIAL

Data are the fuel of AI and ML, including in healthcare, and we are generating more data than ever, with dozens of sensors surrounding every hospital patient and petabytes of self-generated data from consumer medical devices. As just one example, it is now possible to buy a "medical-grade six lead EKG" from Amazon for $149.[19]

Millions of people wear fitness trackers religiously, even to bed. This led to the wonderful Gizmodo headline "Your Fuelband Knows When You're Having Sex."[20] If you burn 100 calories in the middle of the night while taking zero steps, it knows what you're doing. The only question is—who is it going to tell?

Being ratted out by your wearable is not just a hypothetical risk. According to one news report, "a woman caught her boyfriend cheating when his Fitbit activity spiked at 4 a.m."[21]

While that data dump may not have been in the boyfriend's best interest, many experts believe that collecting health data on a mass scale, and analyzing it with AI/ML, may produce the greatest boon medicine has ever seen. Projects like Columbia University–based OHDSI (ohdsi.org) are pioneering a big data approach to medical research.

A 2019 OHDSI-enabled paper published in *The Lancet* "used insurance claim data and electronic health records from 4.9 million patients across nine observational databases, making it the most comprehensive one ever on first-line antihypertensives."[22] It also produced a surprising result—"the most popular hypertension drug isn't the most effective."[23]

AI can be problematic when it can't "explain" how it reached a conclusion. This surfaced in Canada in a legal context when reporters from the *Ottawa Citizen* discovered they could learn the court-protected name of a sexual assault victim by viewing "related searches" on Google.[24] Google officials responded that they hadn't deliberately violated the court's publication ban; however, it was certainly possible that their algorithm, combined with the pattern of user queries, made it possible to see the protected names.

Google also had to pull back on the planned release of more than 100,000 "de-identified" chest X-rays. The National Institutes of Health, a partner in the project, notified Google that some of the images contained personally identifiable information, such as the presence of distinctive jewelry. According to the

Washington Post, "Google's lawyers began raising concerns that possessing and reviewing sensitive health data could create liabilities for the company."[25] Google bowed out of this project but continues to have a keen interest in healthcare technology.

In the U.S. the HIPAA standard for de-identification of protected health information is that "there is no reasonable basis to believe that the information can be used to identify an individual."[26] As the "distinctive jewelry" example showed, small artifacts can yield personal identity information. An even greater risk is that "de-identified" health data sets could be subjected to a technique called "data jigsawing"—combining multiple databases to deduce personal information. In a talk at the DEFCON hacker conference, I showed how Open Government systems could be "tortured" to reveal information that was never intended to be made public.[27]

Aside from the liability of data breach class action suits, of which they are many, healthcare organizations worry about the increasing value of healthcare data on the dark web. According to credit bureau Experian, hackers will pay up to $1,000 for full medical records because they typically contain date of birth, place of birth, credit card details, Social Security number, address, and email addresses in addition to diagnoses. In other words, they are an identify thief's dream.[28]

Applications to help track the spread of COVID-19 have raised vexing data privacy issues. China used mandatory red/yellow/green status QR codes on smartphones to restrict movement, and even deployed creepy talking drones to patrol lockdowns. "Yes, Auntie, this is the drone speaking to you. You shouldn't walk around without a mask."[29]

Western countries generally provided voluntary smartphone apps that could track your contacts, as long as other people's phones also had the app installed. Even then, there was considerable variation in how different jurisdictions treated privacy.

In Utah, the voluntary tracking app recorded the GPS location of the user's smartphone. The Canadian province of Alberta opted for a system that didn't track location. At last count, the ABTraceTogether app had over 200,000 downloads, so many people see this as a civic duty.[30] However, privacy advocates fear that the citizen movement data from tracking apps will be so attractive that governments may be hesitant to see them go away.

There are other looming threats from AI/ML systems to healthcare privacy, such as pills that verify when you take them. Abilify MyCite® dissolves in your stomach and sends a signal to a skin patch, which then reports that you took your medicine. To whom? Well, perhaps the insurance company that paid for your pills wants to make sure that you're not flushing them down the toilet or selling them on the street.

CYBERSECURITY: ALL YOU REALLY NEED TO KNOW

I taught Canada's first computer security course on October 14, 1977.[31] In many decades of watching this field mature, I have concluded that cybersecurity problems stem largely from a failure of imagination on the part of technology designers, and very excellent imagination on the part of hackers.

Systems have gone "haywire" because a program expected a nine-digit number and some joker typed in 200 digits, causing a "buffer overflow." Y2K, largely a nonevent, brought the lack of programmer foresight into the public eye. And, of course, the designers of Zoom never expected people would share meeting links on Twitter, virtually inviting Zoombombers to crash the party.

One of the highlights of hacker conferences like DEFCON, Black Hat, and Germany's Chaos Communication Congress is the revealing of new digital exploits. I have seen a Black Hat hacker make a demonstration ATM machine spew out $20 bills![32] In 2011, a DEFCON speaker took a photo of a "copy proof" Medeco key and reproduced it in plastic.[33] At the 2014 Chaos meeting, a hacker called Starbug used a photograph of the German Defense Minister to reverse-engineer her fingerprint.[34] Another demonstrated that those built-in smartphone cameras could compromise passwords by reading reflections in your eyes![35] White hat hackers play a vital role in keeping technology companies honest by pointing out flaws in their systems, although sometimes the companies are slow to fix the bugs that hackers find.[36]

The clear implication for heathcare technology is that we should try to be smarter than the hackers, and also learn from them as quickly as possible. Fortunately, most of the ones I have met are driven by curiosity and are eager to help. This follows the famous "hacker ethic," which states, "it's not doing what you're not supposed to do—it's doing what you're *not supposed to be able to do*."

There certainly are "black hat" hackers who try to exploit stolen data and monetize zero-day vulnerabilities, and that's what law enforcement should be for. In my experience, most hackers would rather have a round of applause from their peers at DEFCON than the $1,000 they might get from selling your medical records.

ETHICAL MEDICAL TECHNOLOGY

Medical ethics is generally acknowledged to have four key principles:

- *Beneficence* (trying to help the patient).
- *Nonmaleficence* (not hurting someone; e.g., stealing a kidney to save another patient).
- *Autonomy* (respecting the person and obtaining informed consent).
- *Justice* (providing a fair distribution of medical care).

TM would seem to be quite positive in each of these dimensions. After all, its very purpose is to help the patient, and medical professionals are expected to do this in a fair and respectful way. However, inequities can arise. Perhaps some of those earlier-discussed Northern Canadians seen on video could actually benefit from a personal trip to a major medical center.[37] Is it unjust to make them use technology instead of receiving in-person healthcare? Certainly if the video session is hacked, a person's privacy could be harmed. In Canada, a victim may even have a cause of action based on the increasingly popular tort of intrusion upon seclusion.[38]

The use of healthcare AI and ML raises many complicated ethical issues, as explained by the American Association

for Clinical Chemistry (AACC) in a recent publication.[39] They note that the risk to beneficence comes from ancillary use of data collected. Why are tech giants like Google and Apple so interested in getting into this field? A large part of their enthusiasm may relate to what Shoshana Zuboff calls "surveillance capitalism"[40] as they envision more ways to make a healthy profit.

Nonmaleficence could be violated if health data sets are used to actually harm individuals, including by combining them with other identifying data sources.

For autonomy, patients may be asked to trust an AI algorithm that they (or even the creators) cannot fully understand. So the concept of "informed consent" becomes problematic. The AACC recommends banning "black box" algorithms whose results cannot be understood and checked by humans. However, as AI progresses, it may be hard to find a human who is smart enough to understand all the nuances of the system.

Finally, the ethical principle of justice can be violated if technologies like AI-enabled medical care are only available to the rich—like those $5,000 "executive physical" perks given to some CEOs.[41] Reasonable pricing models for this technology should be developed. The AACC states that "[o]ne way to mitigate this risk might be for health systems and patient interest groups to insist on reasonable pricing and distribution clauses in exchange for sharing the patient data needed to develop AI systems."[42] Other experts suggest that the concept of health data ownership should be completely abandoned and replaced with "an obligation to ensure that the data are used for the benefit of future patients and society."[43]

DESIGN THINKING TO THE RESCUE

While the problems set out here seem daunting, we do have a powerful tool to achieve our goals—*design thinking*. It's defined in one source as "an iterative process in which we seek to understand the user, challenge assumptions, and redefine problems in an attempt to identify alternative strategies and solutions."[44]

The magic word here is "iterative." No computer system of any complexity has ever worked perfectly. Even if the initial results looked right, something like a leap year or typing 300 digits into a nine-digit field can trip it up.[45] This is the reason Microsoft has a "patch Tuesday" to fix software glitches (and sometimes introduce new bugs in the process).

Legislators and lawyers will need to play a vital role in this evolution, as privacy and other technology-relevant laws evolve and are tested in court.

There's also a social side—we want to make sure our technology doesn't creep us out!

A decade ago, I wrote about Toto's "smart toilet" that "weighs you when you sit down, checks your body temperature and does on-the-spot urinalysis."[46] Today's possibilities—from tattling pills to smartphones that track your location—make that scenario seem almost benign.

A trifecta is picking the first, second, and third place finishers in a horse race. It's hard—but it can result in a huge payoff to the bettor. We're facing the same kind of challenge as we work to bring healthcare safely into its next evolution. That's what makes it so exciting!

Thomas P. Keenan, EdD, is an award-winning journalist, public speaker, professor in the School of Architecture, Planning and Landscape at the University of Calgary in Alberta, Canada, and author of Technocreep: The Surrender of Privacy and the Capitalization of Intimacy. *He is a Fellow of the Canadian Information Processing Society and the Canadian Global Affairs Institute, serves as Chair of the Information and Communications Technology Council of Canada, and has been an expert witness in a number of technology-related civil and criminal cases.*

ENDNOTES

1. Tom Keenan, *Would Men Show Their Privates on Telemedicine?*, Calgary Herald, May 9, 2020.

2. Derek Thompson, *What's Behind South Korea's COVID-19 Exceptionalism?*, The Atlantic (May 20, 2020), https://www.theatlantic.com/ideas/archive/2020/05/whats-south-koreas-secret/611215/Fbrazian.

3. Janice S. Aikins et al., *PUFF: An Expert System for Interpretation of Pulmonary Function Data* (Stan. Univ., Report No. STAN-CS-82-931, Sept. 1982), http://i.stanford.edu/pub/cstr/reports/cs/tr/82/931/CS-TR-82-931.pdf.

4. *Id.*

5. At the 2003 International Bar Association Conference in San Francisco, participants held a mock trial in which a computer named BINA48, upon learning of plans to shut "her" down and reuse her components, seeks a preliminary injunction to stop the termination. *See* Seo-Young Chu, Do Metaphors Dream of Literal Sleep? (Harv. Univ. Press 2010).

6. Larry Greenemeier, *20 Years After Deep Blue: How AI Has Advanced Since Conquering Chess*, Sci. Am. (June 2, 2017), https://www.scientificamerican.com/article/20-years-after-deep-blue-how-ai-has-advanced-since-conquering-chess (interview with Murray Campbell).

7. While PUFF was genderless, almost all consumer-oriented AI devices have feminine names and voices by default. Apparently, studies have shown the "female voices are perceived as more cordial." *See* Hannah Schwär & Ruqayyah Moynihan, *Companies Like Amazon May Give Devices Like Alexa Female Voices to Make Them Seem "Caring,"* Bus. Insider (Apr. 5, 2020), https://www.businessinsider.com/theres-psychological-reason-why-amazon-gave-alexa-a-female-voice-2018-9. It's also worth noting that HAL 9000, the sentient but rather unhelpful computer in the 1968 movie *2001: A Space Odyssey*, had a male name and voice.

8. Robotics Online Mktg. Team, *Robotic Surgery: The Role of AI and Collaborative Robots*, Robotics Online (July 9, 2019), https://www.robotics.org/blog-article.cfm/Robotic-Surgery-The-Role-of-AI-and-Collaborative-Robots/181.

9. Mauro Annarumma et al., *Automated Triaging of Adult Chest Radiographs with Deep Artificial Neural Networks*, 291 Radiology 272 (2019).

10. *Id.*

11. Jennifer Couzin-Frankel, *Medicine Contends with How to Use Artificial Intelligence*, 364 Science 1119 (2019).

12. BrotherVBrother, *Hilarious Amazon Alexa Fail!!!!*, YouTube (Dec. 31, 2016), https://www.youtube.com/watch?v=-HmAYclRf4g.

13. Ontario Telemedicine Network, Annual Report 2018–2019, https://www.otn.

ca/wp-content/uploads/2020/01/OTNAnnual-Report-1819-final.pdf.

14. *Id.*

15. Kat Jercich, *New Bill Would Mandate Research on Telehealth Regs After Coronavirus,* Healthcare IT News (June 2, 2020), https://www.healthcareitnews.com/news/new-bill-would-mandate-research-telehealth-regs-after-coronavirus.

16. Drew Harwell, *Thousands of Zoom Video Calls Left Exposed on Open Web*, Wash. Post (Apr. 3, 2020), https://www.washingtonpost.com/technology/2020/04/03/thousands-zoom-video-calls-left-exposed-open-web.

17. Simon Woodside, *Why We Should Stop Using Zoom in Healthcare,* Medstack (Apr. 10, 2020), https://medstack.co/blog/why-we-should-stop-using-zoom-in-healthcare.

18. B. Marczak & J. Scott-Railton, *Move Fast and Roll Your Own Crypto: A Quick Look at the Confidentiality of Zoom Meetings*, Citizen Lab (Apr. 3, 2020), https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings.

19. *See* AliveCor, https://www.alivecor.com/kardiamobile6l. There's a cheaper version if you only value your heart at $89. You can even email your results to your doctor. I'm sure they can hardly wait to hear from hundreds of hypochondriacs.

20. A.C. Estes, *Your Fuelband Knows When You're Having Sex*, Gizmodo (July 12, 2013), https://gizmodo.com/your-fuelband-knows-when-youre-having-sex-755620844.

21. Gabby Landsverk, *A Woman Caught Her Boyfriend Cheating When His Fitbit Activity Spiked at 4 a.m.*, Insider (Dec. 11, 2019), https://www.insider.com/woman-caught-boyfriend-cheating-fitbit-fitness-tracker-sex-2019-12.

22. Craig Sachson, *Lancet Paper Shows Most Popular Hypertension Drug Isn't Most Effective, Per OHDSI's LEGEND Study*, OHDSI (Oct. 24, 2019), https://ohdsi.org/lancet-paper-shows-most-popular-hypertension-drug-isnt-most-effective-per-ohdsis-legend-study.

23. *Id.*

24. Andrew Duffy, *Searching for News on Google Can Return Victim and Offender Names Under Strict Pub Ban*, Ottawa Citizen (Sept. 25, 2017), https://ottawacitizen.com/news/local-news/scope-of-potential-ban-breaches-of-secret-identities-through-google-search-broadens.

25. Douglas MacMillan & Greg Bensinger, *Google Almost Made 100,000 Chest X-rays Public—Until It Realized Personal Data Could Be Exposed*, Wash. Post (Nov. 15, 2019), https://www.washingtonpost.com/technology/2019/11/15/google-almost-made-chest-x-rays-public-until-it-realized-personal-data-could-be-exposed/.

26. *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, U.S. Dep't of Health & Human Servs. (Nov. 6, 2015), https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#rationale.

27. Tom Keenan, *How I Torture Open Government Systems for Fun, Profit and Time Travel,* DEFCON 21 (Aug. 1, 2013), https://www.youtube.com/watch?v=eJgTZeUKkhs.

28. Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian: Cybersecurity (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web.

29. TRT World, *China Uses Drones to Warn Its Citizens About Coronavirus*, YouTube (Feb. 3, 2020), https://youtu.be/3-eM4IM-PfY.

30. Tom Keenan, *Contact Tracing Comes of Age—But Where Is It Going?,* Calgary Herald, June 12, 2020.

31. Computer Control and Security, Edmonton, AB (Oct. 13, 1977). The likelihood of anyone challenging this claim decreases continuously from an actuarial perspective.

32. SecurityWeek, *ATM Spits Out Cash at Black Hat—Barnaby Jack ATM Hacking Demo*, BlackHat (2010), https://www.youtube.com/watch?v=fS3Z8Xv-vUc.

33. Christiaan008, *Open in 30 Seconds: Cracking One of the Most Secure Locks in America*, YouTube at 1:22:39, DEFCON 16 (Jan. 22, 2011), https://www.youtube.com/watch?v=iOIRZnafgQk.

34. Alex Hern, *Hacker Fakes German Minister's Fingerprints Using Photos of Her Hands*, The Guardian (Dec. 30, 2014), https://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands.

35. *Id.*

36. Even if technology companies fix their bugs, they may not reach consumers. Months after presenters at DEFCON showed how certain vehicles could be easily hacked, I called car rental agencies to see if they had applied the fix for these possibly life-threatening vulnerabilities. Most said, "No, we're waiting for the cars to come in for their next scheduled maintenance."

37. Anecdotally, many requests for city medical visits from remote Canadians seem to occur during the pre-Christmas shopping period, which has led to providers disallowing shopping trips disguised as medical visits.

38. Heather Gardiner, *Welcome to the New Tort of "Intrusion upon Seclusion,"* Can. Law. (Jan. 20, 2012), https://www.canadianlawyermag.com/practice-areas/privacy-and-data/welcome-to-the-new-tort-of-intrusion-upon-seclusion/271204.

39. Brian Jackson, *Ethics of Al and Big Data in Laboratory Medicine*, AACC: Jan./Feb. (Jan. 1, 2020), https://www.aacc.org/publications/cln/articles/2020/janfeb/ethics-of-al-and-big-data-in-laboratory-medicine.

40. Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (2019).

41. Mark Hendricks, *Executive Physicals: Can a $5,000 Exam Help Improve Your Health and Business?*, Am. Express: Trends & Insights (Jan. 27, 2014), https://www.americanexpress.com/en-us/business/trends-and-insights/articles/executive-physicals-can-a-5000-exam-help-improve-your-health-and-business.

42. Jackson, *supra* note 38.

43. David B. Larson et al., *Ethics of Using and Sharing Clinical Imaging Data for Artificial Intelligence: A Proposed Framework*, 2020. 295 Radiology 675 (2020).

44. Rikke F. Dam & Teo Y. Siang, *What Is Design Thinking and Why Is It So Popular?*, Interaction Design Found. (June 2020), https://www.interaction-design.org/literature/article/what-is-design-thinking-and-why-is-it-so-popular.

45. It is provably impossible to predict what a program will do with every possible input without running it on every possible input. Computer scientists know a variant of this as the "Halting Problem." Undefined Behavior, *Impossible Programs (The Halting Problem)*, YouTube (Nov. 14, 2016), https://www.youtube.com/watch?v=wGLQiHXHWNk.

46. Thomas P. Keenan, Technocreep: The Surrender of Privacy and the Capitalization of Intimacy (2014).