techno creep

THE SURRENDER OF PRIVACY AND THE CAPITALIZATION OF INTIMACY

THOMAS P. KEENAN

techno creep

THE SURRENDER OF PRIVACY AND THE CAPITALIZATION OF INTIMACY

GREYSTONE BOOKS

To my parents, Ruth and Joseph, for allowing me to have white rats and cancer viruses in our basement at the age of fourteen. To the love of my life, Keri, who inspires me every day with her amazing Australian wit and wisdom; and to my wonderful son, Jordan, who bounces ideas around with me like a pro and is navigating his own amazing path in life.

Published by arrangement with OR Books LLC, New York

Greystone Books Ltd.
www.greystonebooks.com

Cataloguing data available from Library and Archives Canada
ISBN 978-1-77164-122-7 (pbk.)
ISBN 978-1-77164-123-4 (epub)

Front cover design by Bathcat Ltd.
Distributed in the U.S. by Publishers Group West

We gratefully acknowledge the financial support of the Canada Council for the Arts, the British Columbia Arts Council, the Provinc of British Columbia through the Book Publishing Tax Credit, and the Government of Canada through the Canada Book Fund for ou publishing activities.

Contents

Preface
Introduction
INTELLIGENCE CREEP
CAMERA CREEP
IMAGE CREEP
SENSOR CREEP
TRACKING CREEP
SENSATION CREEP
BIO CREEP
BODY CREEP
TIME CREEP
GOVERNMENT CREEP
DECEPTION CREEP
PHYSIBLE CREEP
CHILD CREEP
PET CREEP
ROBOT CREEP
CREEP THEORY
ANTI-CREEP
Acknowledgments
Bibliography
References

Figure 1. IBM 1620 computer like the one at Bronx Science. Erik Pitti, via Flickr/Creative Commons Attribution License.

Preface

I wrote my first computer program in 1965, while I was a student at the legendary Bronx High Schoo of Science. Tech pioneers such as Marvin Minsky, Robert Moog, and Martin Hellman once walked it halls, which sometimes reeked of chloroform. In those days, students were actually allowed to perform surgery on small mammals. I remember coming in early one morning to help my friend Mar remove the spleens from several hapless white rats.

Bronx Science had a computer, then a rarity in all but the largest businesses and almost unheard o in a school. It was a cranky card-munching monster that we regarded with a combination of veneratio and lust. In retrospect, jockeying for time on a computer seems like a bizarre hobby for a group of normal teenagers. However, the students at Bronx Science were anything but normal. Eight alumni have gone on to win the Nobel Prize. Two of the Nobel laureates in physics, Russell Hulse and Hugh David Politzer, were in my graduating class. I was in good company.

Access to the school's computer was strictly controlled. Only seniors were allowed near the hallowed IBM 1620 console. We juniors were forced to sit for hours in front of whirring calculators, doing endless numerical analysis calculations and writing down the answers. Our teachers hoped that this would help us appreciate the magical day when we finally got to put our little deck of carefully punched cards into the whirring IBM 1622 Card Reader/Punch. The computer would then do the calculations we had slaved over for the last term in mere minutes, or even seconds.

Driven to get my hands on a computer sooner, I discovered a special youth training program at New York University. If we were willing to give up our evenings and weekends, the folks there would teach us all the computer programming we could possibly absorb. We were even allowed to leave our card decks, secured with rubber bands, for the computer operators to run when they had nothing better to do.

The door of the building that housed NYU's computer had a sign that said "United States Atomic Energy Commission." There was a curtain to shield the IBM 7094 from prying eyes when it did secret work. The Soviets had launched Sputnik in 1957, leading to fears that they would dominate the world from space. The 1962 Cuban missile crisis had us doing air raid drills in school. Clearly computers were going to play a role in saving America, and we were being trained to play a part in that drama.

Under the leadership of professors including Max Goldstein and Jacob T. ("Jack") Schwartz, and coached by a kind-hearted and energetic NYU researcher named Henry Mullish, there were no limits to what we could accomplish. We created whole new computer languages, fixed bugs in existing ones and wrote emulators for computers that were still on the drawing boards. I wound up programming everything from the statistics for numerous PhD dissertations to particle physics calculations to some of the structural engineering data for the original World Trade Center. I earned my keep on that last project by catching a glitch that might have caused the two 110-story towers to collide in high wind conditions.

Back then, computers spat out their results in 132 column-wide format on oversized continuous sheets of paper. When I pulled out a printout while riding the Bx40 cross-town bus in the Bronx, I always got strange looks from the other passengers. I was proud that I had something special and almost magical in my hands. I now realize they probably thought I was a very creepy kid.

Years of being a computer programmer, a computer science professor, and a technology journalis have helped me realize that almost every new technology can be misused and often become deeply disturbing. In 1984, I had the great fortune to co-write and host a CBC IDEAS series called *Crimes o*

the Future, in collaboration with Dr. Duncan Chappell, then head of the Criminology Department of Simon Fraser University; and Dave Redel, a very talented CBC Radio Producer.

Those programs marked the first time many people heard about identity theft, except perhaps in the context of someone going to a graveyard to copy the name and birth date of a deceased infant. We talked about crimes that have now become real, such as trafficking in human body parts, and others that are only now surfacing, like "wireheading"—the direct stimulation of the pleasure centers of the brain. Back then, we had to use the work of science fiction writers like Larry Niven and Spider Robinson to introduce this intriguing practice. Today there are detailed, instructions for brain self-stimulation on the Internet.[1]

For almost five decades now, I have been watching as everybody else gets on the tech bandwagon sometimes adroitly, sometimes clumsily, and often without fully understanding the implications of what they are doing.

This work has taken me to conferences like DEF CON; Black Hat; Computers, Freedom, and Privacy; and led to unexpected adventures such as being allowed to scrub in on a liver transplant operation. I have had the privilege of talking to thousands of academics, visionaries, and technology creators, and come away with the strong sense that we need to raise the bar in our thinking about technocreepiness, and sooner rather than later.

Over half the people on that Bronx bus today would now be glued to their smartphones, connecting with friends, checking sports scores or enjoying celebrity gossip. Would any of them be thinking about the next chapter in technology, and how it is going to change their lives?

This is a book about the creepy pioneers of technology: what they are doing and why we need to know about it. In the pages that follow we will go on a journey into some of the disturbing ways our lives are unfolding, often behind the scenes and without our knowledge or permission. Not all of these incursions are necessarily bad. The benefits of knowing you are prone to a certain disease, for example, *might* outweigh the risks of having genetic tests on your medical record. And what seems creepy today may be the accepted norm in the future.

Still, there is this nagging feeling that decisions we make today may come back to haunt us in the future, in ways that are hard to envision. Yet that is precisely what we should be doing.

Introduction

Modern technology is not what it seems. Or rather it is much more than it seems. Digital wheels are turning in the background that most people do not even know exist. Increasingly, we are getting an uneasy feeling about this … a sense that things are not quite what they seem.

So much is happening that is out of our view and beyond our control. Like a network of mushroom spores sending out subterranean tendrils to silently exchange genetic material, our technological systems are increasingly passing information back and forth without bothering to tell us. They are parsing and analyzing it to squeeze out the deep meaning of what we say and do, sometimes before we are even aware of our own intentions.

Technocreep is quietly but relentlessly invading our daily lives:

- You use your smartphone to take a photo, and it auto-uploads it to Facebook. Without your knowledge, metadata such as the type of camera you use and the precise location where you took the photo is also being uploaded. Facebook may remove that information before making your photos public, but the company certainly has access to all of that metadata for its own purposes. Facebook now has the world's largest known database of personal information and photos, many of them conveniently labeled with your real name. How deep is the analysis of your words and photos by Internet giants like Facebook and Google? According to an article in *Wired*, the computers at Facebook can use artificial intelligence to tease out the emotions in your rambling and figure out when you are being sarcastic.[2] That same article says that Google can distinguish the facial features of a cat from a human.
- You decide to check your email, which, like most people, you are now getting for free from a provider like Google, Yahoo, or Microsoft. Hmm, no new mail has been delivered for the past few hours. Do their servers get backed up like the post office at the holidays? Or is something more sinister going on? Is your mail being siphoned off for some sort of deep-level human or computer analysis? Given the revelations of Edward Snowden and others, your concern might be justified. What should certainly disturb you is the fact that you have no way to really know how your web-based email is processed, and virtually no tools to investigate it; while others seem to have many tools to investigate you.
- Before heading to bed, you peruse the electronic catalog of an upcoming estate sale, lingering on the image of a nice chandelier. An advertisement for the website www.chandelier.com pops up on your screen. How did they know what you were thinking about? Perhaps it was because the sale image was saved as chandelier.jpg. But perhaps not. Image recognition technology is progressing at an amazing pace. Again, the wheels are turning in the background in a creepy fashion.
- Late at night, you hear the hard drive whirring on your computer. The monitor is flickering even though nobody is using it. Perhaps it makes a few of those strange "bonging" sounds that signify someone is sending you a message. You look. But there is nobody there, and the computer, as if sensing your presence, has ceased its frantic activity. All is calm. But you are not sure if it was Microsoft doing software patches, a hacker trying to steal your information, or … something else.
- Bars in several cities have installed cameras that silently watch their clientele and make inferences about them from their physical characteristics. Armed with the free smartphone app

SceneTap, prospective patrons can check out how full the place is ("chillin" to "hoppin") as wel as the average age and percentage of males and females there.

- "Suggestion algorithms" are popping up on shopping and social networking sites. It is no surpris that Amazon is trying to sell me the last few things I price-checked there (and bought elsewhere But when it suggested "adult size disposable diapers" as a good purchase for people buying certain video games, did it "know too much"?
- Google's Regina Dugan has suggested with a straight face that you may soon swallow a passwor pill or sport a digital tattoo to log on to computer systems.[3] Both ideas are technologically feasible right now, but should our employer be allowed to brand us or make us take a pill?
- Next generation wearable computers such as Google Glass may start regularly tracking where you are looking.[4] That information will then be sold to advertisers and others who are seeking a window into your mind. Based on where your gaze lingers, they will suggest things you want to buy even before you know you want them.
- Your phone may listen for audio cues about where you are. Is that a football stadium announcer hears? Perhaps you would like a discount coupon for the team's store, or, if you are slurring you words, a connection to a "drive me home in my car" service.

Perhaps you will seek refuge from all this invasive technology in some nostalgic low tech activity lik attending a rock concert. We will still have those in the future, as people clamor for the "live experience" in a world with unlimited digital media access. But the fiftieth anniversary Woodstock concert will probably be a lot different from the original one in 1969.

At Woodstock 2019, you may be swatting away disposable flying robot cameras that people have launched to catch a better view of the performers. Folks all around you will be pushing the "find my friends" button, revealing their exact location at the concert venue. Unlike today's friend finder apps the 2019 version may also tap into their brain waves and body chemistry to decide if they are interested in joining you for some food, or perhaps something else. Yes, babies will be conceived at Woodstock 2019 just as they were in 1969.

If you have broken some minor rule like forgetting to renew your vehicle's license, you will com back at the end of the show to see your "smart license plate" displaying "EXPIRED" where the number should be. Should you decide to buy a souvenir T-shirt, your every move will be tracked by cameras that make uncannily accurate estimates of your age and gender, and then predict your buying habits.[5] They may even recognize you by your face or change the prices based on the color of your credit card, which it will be broadcasting to the world.

Should you seek medical help at Woodstock 2019, you will almost certainly receive tests and treatments tailored to your unique genetic makeup. Dr. Leroy Hood, the biologist who pioneered automated DNA sequencing, describes what you should expect at the Woodstock 2019 first aid tent. "We'll be able to prick your finger," he says, "and take a droplet of blood and make ten thousand measurements that tell us about a gazillion different things that may speak to why you have apparent cardiac pain. There'll be very powerful imaging devices that can probably be done at Woodstock that could look at the brain or look at the heart."[6]

Hood also believes that this type of personalized medicine will come down in cost very rapidly. "My own prediction," he says, "is with third generation DNA sequencing … the genome will cost $100 and we'll be able to do it in fifteen minutes." That price drop, from the current level of thousands of dollars, should put your mind at ease. After all, there will be no way to skip out on your bill at this medical facility. They will have your DNA sample.

Unlike in 1969, when misadventures with psychedelic chemicals accounted for many visits to the medical tents, the Woodstock 2019 medics may be treating the after-effects of electronic stimulation of the pleasure centers of the brain. And just as crowdfunding sites are starting to determine which products are manufactured by online consensus, Woodstock's organizers may be able to tap into the "hive mind" of concert-goers to keep the show moving at just the right pace.

If you cannot make it to the live event, there will be ultra-high-resolution videos to enjoy, streamed directly into your retina or perhaps even your brain. Organizers will probably use big data analytics and artificial intelligence to choose the lineup of musicians. That is how Hollywood already decides which television shows we are most likely to watch.[7]

This book is about the unseen ways in which technology is already changing our lives. We will visit the hotel suites at the DEF CON and Black Hat conferences, where hackers attack circuit boards and tweak software late into the night. We will go into the online nooks and crannies where digital exploits are secretly shared. We will even examine a kids' toy that frightened the National Security Agency so much that it was banned from their building. You will learn why you might want to avoid certain kinds of medical testing and why your online presence will definitely outlive you, unless the "transhumanists" are correct and the first immortals are already living among us.

Many people believe that these disturbing technologies are confined to the Internet and that if the are careful, or even avoid online activity altogether, they will be safe. But the technologies that will truly change our lives will be in our cars, our streetlights, our hospitals, and even inside our brains an bodies. Our favorite watering holes, even our pets and our children, are being infested with technocreepiness.

The general public learns about creepy technologies episodically. A whistle-blower unveils whole areas of government or corporate snooping. A probing journalist figures out how big data can be used to link together nuggets of your life to create a chillingly accurate portrait of you. A scientist works backwards from a DNA sample to infer the most likely surname of the person it came from.[8] Perhaps you receive a particularly astute yet unsettling suggestion for a new contact on Facebook or LinkedIn and wonder how they did that.

Every new technology eventually attracts calls to restrict or regulate it, and often to find a way to turn it into a revenue stream and make it taxable. But the flow is becoming too fast, too diverse, and too imaginative for lawmakers to keep up.

We will always have new innovations, and people will find ways to misuse some, and to combine them in unanticipated ways. Some ideas will pass into oblivion like the pernicious RottenNeighbor.com. For a while, this website let you anonymously badmouth folks whose dogs allegedly pooped on your lawn or falsely label the guy down the street as a sex offender. Companies were not exactly eager to advertise on RottenNeighbor.com, and it now sits, dormant, though still registered and presumably ready to rise again if a viable business model suddenly appears. The "uncensored people reviews" at dirtyphonebook.com continue to provide an outlet for this kind of personal attack.

Creepiness is an elusive concept that taps into our primal fears and assumptions about the way things are and should be. Sigmund Freud pondered it, suggesting that creepy things, with part of their true nature hidden, remind us of our own deepest secrets and guilt over repressed impulses. Edgar Allan Poe achieved heights of creepiness in his short stories by playing on our fears of being buried alive or catching the plague.

Filmmakers often seek the fine balance that will send the audience away wondering darkly about character's true nature and motivation. Culture blogger Sarah Dobbs explains that movies can be sca

with loud noises and sudden moves, but that truly unsettling cinema is a lot harder to achieve.

"To be one of the good horror movies," she writes, "a film needs to establish a certain atmospher it needs to draw you in and make you care. It needs to give you something to think about when you're trying to drop off to sleep at night; to make you wonder whether that creaking noise down the hallwa was just the house settling, or something lurking in the shadows. Creepy stays with you. It gives you goosebumps."[9]

Clowns, dolls, ghost stories, and even the words from the mouths of our young children can fascinate us in unsettling ways. The closer something is to our hearts and our highest values, the mos disturbing it can be.

A famous discussion on the social news site reddit asked, "What's the creepiest thing your young child has ever said to you?"

Here are two of the more disturbing examples:

I was tucking in my two-year-old. He said, "Goodbye, Dad."
I said, "No, we say goodnight."
He said, "I know. But this time it's goodbye."
Had to check on him a few times to make sure he was still there.
/u/UnfortunateBirthMark

And

When I was about three we had a cat that had stillborn kittens.
I asked my father if we could make crosses for them, which he did.
As he was making them I asked: "Aren't those too small?"
Dad: "What do you mean?"
Me: "Aren't we going to nail them to them?"
Dad (after several moments' silence): "We're not going to do that."
Me: "Oh."
/u/Tom_Zarek[10]

Cute? Innocent? Perhaps. But the creepiness stayed with these people long enough for them to share i on reddit. The fact that this thread is now up to around 15,000 comments speaks to our fascination with the *unheimlich*, a German word that literally means "the opposite of what is familiar or home-like." By thinking about what unsettles us the most, we are able to confront and understand our greatest fears, and try to make rational decisions as citizens, software designers, creators, parents, an consumers.

So, what is creepy? We know it when we see it. The hairs stand up on our neck or we ask, "How d they know that?" Creepy things make us question our assumptions, and lie awake, wondering "what if?"

My study of hundreds of technologies that are creepy in various degrees has revealed some common factors that make people uneasy. At the end of this book, we will explore these "dimensions of technocreepiness" in the hope that we can avoid them in the future. We will even do a bit of "creep proofing" to, as much as is humanly possible, protect ourselves from the worst ravages of invasive technologies. But for now, let us let those hairs do their job. We will begin our journey into

technocreepiness at a rather unlikely place—the New York Public Library.

Intelligence Creep

There are twenty-nine steps from the corner of 41st Street and Fifth Avenue to the front entrance of th New York Public Library. I know this because, in the mid-1970s, I lugged a radio station's tape recorder up every one of them. I might as well have been carrying a television set. Back then, "portable" meant that something had a handle. I was there to interview the keeper of an amazing new technology—the Kurzweil Reading Machine.

Billed as an aid to the blind, this bulky contraption was the world's first functional text-to-speech synthesizer. Walter Cronkite used the machine to sign off on his January 13, 1976 newscast. I typed u a piece of paper with "For CBC Radio, this is Tom Keenan in New York." The machine rattled this o for me in the same mechanical monotone that we now associate with the hacktivist group Anonymou

I then asked the librarian, "What kind of things do people bring in to read on it?"

"Mostly pornography," he replied.

I thought I had heard him wrong. He explained that "if somebody wants to hear a textbook on American History or something, there are plenty of volunteers who will read that. We're seeing book like *Lady Chatterley's Lover*, *The Story of O*, that sort of thing."

A lot has changed since my first encounter with the Kurzweil Reading Machine. Instead of luggin a bulky tape recorder, I can now push a button on my smartphone and safely store my interview in th cloud. If I want to know how many steps I will face at the New York Public Library, I can simply count them on Google Street View. Anyone with Internet access can find all the pornography they could possibly want, and have it read to them in whatever exotic voice they desire.

The abundance and variety of Internet pornography illustrates a concept that Cullen Jennings, one of my former students and now a Cisco Fellow, expressed very well. "No matter how liberal or broad minded you are," he once said, "I guarantee I can find something on the Internet that will instantly offend you." It is a small leap from "something that will offend you" to "something that will creep you out."

Even though I have seen a lot of bizarre things since the 1970s, the image of tumescent guys hooked up to the Kurzweil Reading Machine at the public library has stuck with me, along with the gadget's monotone voice.

A good friend and I used to split the generous "lead fees" which a certain national tabloid paid fo ideas that turned into stories. Driven by empty wallets, and armed with a bottle of Jack Daniels, we could spin off quite a few plausible if sensational ideas in an evening. Of course, a tabloid tale is not publishable story without a reputable expert to support it. This paper had a helpful list of "trained seals" who, for a fee, would happily confirm UFO sightings and authenticate photos of fictional monsters. Yet they had a big gap—they needed a bright young computer science professor, which wa precisely my line of work.

Soon I came to be quoted on fantasy technology stories like "an amazing implanted chip will someday measure your caloric intake and release an appetite-suppressing hormone." That feature attracted bags of mail from people desperately seeking to help me test this rather wacky idea. I sent the letters back suggesting that they look into some diet and exercise plans.

Perhaps I should have told them to wait. An article in the 2009 issue of *MIT Technology Review* describes a "small, stick-on monitor no bigger than a large Band-Aid" that can accurately monitor your caloric intake.[11] Some smart scientist will undoubtedly invent the appetite suppression techniqu and make our fictitious dieter's dream patch a reality.

In that weekly tabloid, I also mused that "someday computers will speak to you in the voice of your choosing. It might be Marilyn Monroe's or Clark Gable's or the voice of your long-dead mother." Since then, science has shown that the sound of your mother's voice indeed does have a profound physiological effect on you.

In studies of mother/daughter dyads, Leslie Seltzer found that hearing Mom's voice raised girls' oxytocin levels, calming them down.[12] Email and SMS messaging did not have the same effect. Som have even speculated that an artificially intelligent program that sounded like your mother, used her favorite expressions, and had an intimate knowledge of your life story, could be a powerful way to calm, interrogate, or even control you.

Back in 1966, Massachusetts Institute of Technology professor Joseph Weizenbaum unleashed ELIZA onto the world, hoping to illustrate the fundamental differences between human and compute brains. A fairly simple "chatterbot," ELIZA could mimic the conversation style of a Rogerian psychotherapist, faking the answers when it did not understand what you just said.

Weizenbaum observed that a session with a psychotherapist was one of the few environments where it was perfectly acceptable to turn a question back on the speaker, or provide a canned respons like "So, how does that make you feel?"

Although Weizenbaum intended ELIZA to be a parody with a point, many people enjoyed pourin out their personal problems to the program. Some even said they preferred it to a human therapist. When Weizenbaum told his secretary, who had been using the software, that he had access to the log of all her conversations with ELIZA, she was outraged at this invasion of her privacy.[13]

ELIZA got herself into some humorous situations. In the age before massive hard disks, compute data was usually stored on 2,400-foot reels of magnetic tape which had to be manually mounted by a operator. The tape mount request came up as a flashing message on the operator's console.

However, some of MIT's computers did not have a human operator available. Pranksters configured one of them to use ELIZA to respond to operator requests. "Can you please mount a tape for me?" was met with "Is it because of your mother that you want me to mount a tape for you?"[14] Profanity usually ensued from the hapless human.

The idea of programs that can mimic human conversation has spawned some creepy chatterbots a major companies. In 2006, the Coca-Cola Bottling Company of Atlanta, GA, "hired" a virtual representative named Hank. Hank was intended to, among other things, deflect phone calls to the company's main switchboard from students doing reports on the history of Coca-Cola. He straddled the line between being a computer program and a person quite adroitly for his era.

I had some great talks with Hank. We discussed his personal life ("virtual representatives are not allowed to have relationships") and he vehemently denied that Coca-Cola has ever contained cocaine

Other people also tormented Hank with questions like[15]:

Q. Do you like snorting coke?
A. Of course! I like all of the products of The Coca-Cola Company.

Q. Are you a Mormon?
A. We are not in a position to comment on the ownership of stock. The holdings of our share owners are confidential. In accordance with our current governmental regulations, however, we

include in our annual proxy statement a list of those share owners who are beneficial owners of five percent or more of our company stock, and the Mormon Church is not among them.[16]

History does not record when Hank was downsized from a full-fledged virtual representative to a "frequently asked questions" webpage.[17] That seems to be all that is left of him today, though he is still wearing his trademark telemarketer headset.

If you could talk with Hank about such personal matters, why not unburden your venal and even mortal sins to a piece of technology? On-line confession does seem to have some kind of creepy visceral appeal to people. In 1984, an art project called "Interactive Catholic Confessional"—based loosely on ELIZA—was put on display. "Visitors entered a confessional space, knelt before the computer and went through the process of Catholic confession," according to a posting at the University of Nevada at Reno. "The computer gave each user an appropriate penance for their sins."[1

The concept of computerized confession is still with us. In 2013, a Jewish congregation in Florida urged its members to atone for their sins through anonymous, but very public, tweets which would scroll by on a screen during the Yom Kippur services.[19]

On a more secular level, reddit has a whole subreddit called r/confession, and entire websites like www.truuconfessions.com ("your anonymous best friend") thrive on this compulsion to share guilty secrets. Here, you can learn who is lusting after his cousin's wife and who "kicked a child (who probably deserved it)." These posts make fascinating reading, but of course their real purpose is catharsis for those who write them. An amazing number of people seem to spend a lot of time poring over these stories, "upvoting" and "downvoting" them, and adding their own commentary. In one sense it is a new way of communicating with a higher power, even if this higher power is only a transient, anonymous online community.

The line between machine and human thinking is definitely blurring, as is well illustrated by the triumph of IBM's Watson over the best human Jeopardy players. Virtual assistants like Apple's Siri and Microsoft's Cortana are mining our smartphones and emails to do some of our thinking for us.[20] We can feel the hot breath of our technology pushing us relentlessly towards that much-touted "singularity"—the day when our creations will be smarter than us in ways that really count.[21]

In the mid-1800s, Augusta Ada King, Countess of Lovelace, studied the work of Charles Babbage who designed a precursor to modern computers. Because she wrote down the steps to compute the Bernoulli numbers on Babbage's never-constructed Analytical Engine, Lovelace is often called the first computer programmer.

She is also known for her famous "Objection" to the idea that a machine can possess creativity. "The Analytical Engine has no pretensions to *originate* anything," she wrote in 1842. "It can do *whatever we know how to order it* to perform"[22] (her italics).

If she were alive today, Lovelace might have trouble maintaining her position as Watson trounce her in her choice of intellectual games. But we do know that, putting aside quantum computers, neura networks, and other specialized technologies, mainstream computers still sequentially execute instructions that were designed by their human masters. If Lovelace's Objection is as true as ever, wh do technologies do things that amaze us and give us creepy spinal shivers?

One explanation of this apparent paradox is that many computer programs have already surpasse the comprehension of any *one* human mind. This was actually true of the operating system, OS/360, made for IBM's mainframe computers in the 1960s and 1970s. It had so many modules and complexities that it took a team of systems programmers to build it, and nobody purported to know

every inch of it. Mix in the creative input of today's very bright designers and programmers, and you get a continuous stream of technologies that amaze, delight, confound, and, increasingly, disturb or even frighten us.

Sometimes we have trouble detecting the boundary between machine and human intelligence. Most people recognize that the "Recommended" suggestion list from Amazon.com comes from a robot. But what about the earnest email appeal from a friend who claims he is stranded abroad witho funds. The sender seems to know intimate details about your mutual relationship. It is probably a nasty robo-scam, but how can you be sure?

In his signature essay on the subject, Sigmund Freud tackled the psychological aspects of our discomfort with things that may or may not be human. Using the example of the doll in the first act o Offenbach's opera, *Tales of Hoffman*, he acknowledges that "doubts whether an apparently animate being is really alive" can invoke The Uncanny. Freud goes on to suggest that what we truly dread her is an Oedipus-style gouging out of our eyes, or, this being Freud, a symbolic castration.[23]

Japanese robotics professor Masahiro Mori coined the term "uncanny valley effect" to explain why we become uneasy when non-human things exhibit human-like behavior.[24] Perhaps nothing embodies the spirit of the uncanny valley better than BINA48.

Figure 2. (top) BINA48 from the front. Courtesy of Robert Koier.
Figure 3. (bottom) BINA48 from the rear. Courtesy of Terasem Movement Foundation.

Martine Rothblatt, a serial entrepreneur, lawyer, and researcher, has created an extremely lifelike humanoid robot in collaboration with robotics engineer Dave Hanson. In addition to having a convincing and expressive face made of a polymer called "Frubber," BINA48 has an uncanny ability to display human mannerisms. *New York Times* reporter Amy Harmon, sent to Vermont to interview BINA48, reports a profound moment as BINA48 looked her in the eyes and said "Amy!"

“Maybe it was the brightening of the sun through the skylight enabling her to finally match up my image with the pictures of me in her database,” Harmon writes. “Or were we finally bonding?” The spell was broken by BINA48’s jarring next remark, which was to change the subject: “You can ask me to tell you a story or read you a novel.”[25]

BINA48 has cameras in her eyes and is equipped with face finding and facial recognition software. As their cost plummets to virtually zero, digital cameras are turning up almost everywhere. They now seem to be present at the best, worst, and creepiest moments of our lives.

On April 19, 2013, law enforcement agents used a thermal imaging camera, combined with a tip from a citizen, to locate Dzhokhar Tsarnev in the aftermath of the Boston Marathon bombings. The image of a human form crouched under a tarp sped around the globe. The imaging technology was praised for leading to the result almost everyone was hoping for: the live capture of a desperate fugitive.

Figure 4. Fugitive Dzhokhar Tsarnev, hiding under a tarp. Courtesy of Massachusetts State Police Air Wing.

Thermal imaging cameras are not new. They have been used for years by firemen (who look for cool spots since burning walls are much hotter than trapped humans) and by house inspectors probing for heat-wasting leaks.

They also play a role in tracking down marijuana grow-ops and finding people and objects hidden in walls and vehicles. Yet, suddenly thermal imaging was front page news, seeming to give law enforcement superpowers. From their helicopter, the Massachusetts State Police found a needle in a haystack, using what seemed like a kind of x-ray vision.

Regular cameras also played a role in this investigation, as agents pored over masses of amateur cell phone video and surveillance camera footage. The cameras that yielded the best pictures were th ones mounted on the Lord & Taylor store and the Forum Restaurant at 755 Boylston Street in downtown Boston.[26]

I walked that very stretch of Boylston Street a few months earlier. While those cameras were not hidden, they certainly would never catch your attention. Yet they provided vital evidence. After siftin through all the images, authorities published photos of suspects they dubbed “Black Hat” and “White Hat,” asking for the public’s help.

The “go public” strategy worked, and Dzhokhar Tsarnev was soon apprehended alive. Despite thi outcome, some academic researchers called the Boston Marathon bombing case “a missed opportuni

for automated facial recognition to assist law enforcement in identifying suspects."[27] Joshua C. Klontz and Anil K. Jain of Michigan State University did an after-the-fact simulation using the Bosto suspect photos and a database of one million mugshots released under Florida's "sunshine" law. They stirred in photos of the Tsarnev brothers taken on various occasions such as after a boxing match in 2009. Using commercial facial recognition software, they had some success in matching them, including a "rank one" matchup between a bombing scene photo released by the FBI and a high schoo graduation photo of Tsarnev.

The researchers acknowledge that neither of the commercial facial recognition systems they teste is ready for routine deployment in law enforcement applications, largely because of issues with different poses, resolution, and factors as simple as wearing sunglasses. However, you can be sure tha work on improving facial recognition for law enforcement is moving full speed ahead.

Soon after the Boston Marathon bombings, Joseph Schuldhaus, vice president of information technology Technology for Triple Five Group, which runs the sprawling West Edmonton Mall and as well as Minnesota's Mall of America, suggested that video analysis is going to become even more important in fighting crime. "I think we're going to see the further miniaturization of algorithms at the edge of the device," he told IT World Canada editor-at-large Shane Schick, "and what I mean by that is when the video comes into the camera these algorithms are going to help law enforcement better process that information, much like when you use Shazam to identity a song."[28]

Schuldhaus clearly believes that the public safety and security advantages of surveillance camera outweigh the risks they pose to privacy. Others are not so sure; but this has not stopped cameras, both public and private, from proliferating around the world.

According to a report in *Forbes*, "In the United States, it is estimated that there are 30 million surveillance cameras, which create more than four billion hours of footage every week."[29] They are also sprouting a lot of intelligence and new functionality. Their images are processed, in real time, to highlight suspicious packages at airports, to discover people who go where they are not supposed to be, and, even, as proposed by some Japanese researchers, to catch kids smoking in the schoolyard.[30]

For many years, a conference called Computers, Freedom, and Privacy featured a post-conference tour of the host city's surveillance cameras. I vividly remember going on the tour of San Francisco in 2004. We stopped after we found about a hundred cameras peering down at unsuspecting people in Union Square and other public venues.

Dedicated volunteers from the New York Civil Liberties Union walked around Manhattan in 1998 noting camera locations, producing what they called "a comprehensive map of all 2,397 surveillance cameras in Manhattan." When they re-did the same study in 2005, they "found 4,176 cameras below Fourteenth Street, more than five times the 769 cameras counted in that area in 1998."[31]

They are fighting an uphill and ultimately hopeless battle. Modern surveillance cameras can be tiny, totally wireless, solar powered, and cost a few dollars. Good luck spotting one of those pointing out of a window or hiding in the pore of a ceiling tile.

It is hard to deny that the presence of video cameras in public places has deterred some criminals and solved or prevented certain crimes. In one case, a bandit robbed a local wholesale club, and was caught on the surveillance camera. A simple scan through the membership records turned up a match for his photo, yielding his name and home address.

The heavy camera coverage of New York's Times Square is credited with helping police thwart the plot to detonate a bomb there in 2010. However, just as in the Boston Marathon bombings, a tip from a citizen also played a major role. Once, while watching a camera pointed at Times Square, I sa an entire drug deal transpire in plain sight.[32] I managed to capture several screen shots and use it as a

example of people who obviously did not realize they were being watched. Or who did not care.

Do cameras really earn their keep as crime fighters? The best data on this comes from the United Kingdom, which has had extensive camera coverage for over a decade. The results are not as encouraging as camera advocates would like us to believe. A 2009 Scotland Yard report estimated th only one crime was solved per year per thousand cameras.[33] The resulting bad press for cameras was met with claims in 2010 by the London Metropolitan Police that they were actually able to solve six crimes a day with camera evidence.[34] Commentators scoffed that most of them were probably jaywalking.

A recent scientific review of various crime prevention techniques looked at thirty-six U.K. studie ten in the U.S., and one in the Netherlands. These researchers found that "there is little evidence that the following reduce fear of crime: street lighting improvements, closed-circuit television (CCTV), multi-component environmental crime prevention programs, or regeneration programs."[35] Many securities cameras are, as Bruce Schneier famously puts it, "security theatre."[36]

A number of motor vehicle registration operations now run an applicant's photo through facial recognition to see if a driver's license has already been issued to the owner of that face. In British Columbia, Canada, the government-run monopoly auto insurer, Insurance Corporation of British Columbia (ICBC), uses facial features including the distance between the eyes as well as cheekbone geometry to root out fraud. Their photo database is of great interest to law enforcement, but there are some thorny privacy issues there.

On June 15th, 2011, downtown Vancouver was engulfed in riots after the home team lost the fina game in the Stanley Cup hockey series. People were stabbed, police officers were injured, and there was extensive property damage. Digital devices helped to feed the violence, as rioters reacted to the presence of media and personal cameras. However, digital photos also played a key role in tracking down the offenders.[37]

British Columbia's Information and Privacy Commissioner, Elizabeth Denham, had to decide if using the ICBC's motor vehicles registration database to try to identify offenders would violate the province's privacy laws. She ruled that it was acceptable for the police to provide candidate images t ICBC for possible matching. However, a court order would then be required for the matched-up resul to be revealed to the police.[38]

Police in Vancouver also put out an appeal to the public to assist in the massive post-riot investigation. They set up a special website, riot2011.vpd.ca, with photos of "people who are alleged to have committed criminal offences." The public was offered a simple "click and identify" system t provide information.

Did it work? In July 2013, two years after the riot, the Vancouver Police Department (VPD) announced that they had recommended charges against 352 alleged rioters for 1,204 offenses. The accused were as young as fourteen years old. As an example, the report describes three high school friends from Victoria, British Columbia, who "were captured on video committing multiple crimes throughout the night, including break-ins to four separate businesses." VPD Superintendent Dean Robinson says they are not yet finished hunting down suspects, and "those rioters out there that believe they can wait us out and hide with anonymity, we will find you and you will be brought to justice."[39]

There are a number of reasons why the Vancouver Police Department turned to the public for hel One is just good public relations—hooligans trashing the city's downtown does not sit well with mos law-abiding citizens. Also, some of the demonstrators had no criminal record, and may have been too young to be in the motor vehicles system.

While the surveillance camera and cell phone videos used by the VPD were certainly helpful, they are nowhere near the state-of-the-art in surveillance camera technology. A remarkable photo of the crowd on Georgia Street taken a few hours before the riot was posted by a company called Active Computer Services. It is actually a composite image of 216 high-resolution photos stitched together, and it reveals an uncanny level of detail.[40] You can zoom in from the massive scene to identify individual faces with ease. Active Computer Services has a particularly telling motto on their home page ("I spy with my little eye … ") and they tout the "forensic science" applications of their technology.

According to Charlie Savage in the *New York Times*, scanning for a wanted face in a crowd is still a tough computer science problem.[41] However, Savage writes, progress is being made: the U.S. government–backed Biometric Optical Surveillance System (BOSS) works with two cameras, equipped "with infrared and distance sensors. They take pictures of the same subject from slightly different angles. A computer then processes the images into a '3-D signature' built from data like the ratios between various points on someone's face to be compared against data about faces stored in a watch-list database."

The Department of Homeland Security ran a test of BOSS in September 2013, using it to scan about six thousand fans attending a hockey game in Kennewick, WA. The faces of twenty volunteers were placed in a database. The challenge was to find them among the hockey fans, at a distance of fifty to one hundred meters, quickly enough so that if any were terrorists they could be located and intercepted. The results have not yet been disclosed.

Several commentators have noted that this type of surveillance system is often launched for crime fighting or anti-terrorism purposes, but people quickly find other uses for it, including commercial ones. The day is not far away when the kid selling soft drinks at a stadium may pass you a note that says your car's lights are on, having linked your face in the crowd to your license plate. They might even figure out a way to charge you for that service.

While this BOSS technology is not yet operational, experts say it will be deployed within five years. Privacy advocates suggest that we need to make rules now about how it can be used in the future, or we will simply default to ubiquitous surveillance.

The FBI, the Department of Homeland Security, and the U.S. State Department are very enthusiastic about facial recognition. According to Brian Merchant, writing for *Motherboard*, "the Department of State currently runs one of the largest facial recognition operations in the world. It uses a database of 75 million photos or so to cross-check visa applications."[42]

While we hear a lot about the prevalence of cameras in the U.S. and the U.K., another country is on track to become the world leader in video surveillance. China is already estimated to have one surveillance camera for every forty-three of its citizens.[43] I have been taken into a secret monitoring center in a major Chinese city where operators watch a gigantic wall of monitors covering every major intersection. The Chinese have a significant home-grown surveillance camera industry, ironically boosted by the United States, which slapped export restrictions on surveillance technology in 1989. That fueled China's own research and development in this field.

Private use of facial recognition technology is also growing daily. The contours of this expansion were neatly summarized by *Motherboard*'s Jordan Keenan, who wrote, "If you use social media, have a driver's license, shop in stores, and walk in public, chances are good that your faceprint will soon be assigned to your identity, and eventually be used on a daily basis to build a profile of you at a level of detail you hoped would never be possible."[44] Improving facial recognition is also the reason you have to maintain such a stern expression for your passport and visa photos.

On August 8, 2000, a woman wearing a toque and dark sunglasses entered a Safeway store near downtown Calgary, Alberta, Canada, pushing a toddler in her shopping cart. She wrote a note addressed "To Whoever finds my son," wheeled him into the cookie aisle, and simply left the store. According to media reports, the two-year-old kept saying "where is my Mommy?" but she was nowhere to be found.[45]

Police were called, and appealed for the public's assistance on the television news. When the mother did not come forward, Alberta's Minister of Children's Services ordered publication of this photo, shown here at reduced quality to preserve privacy.

Figure 5. Woman in Safeway with baby. Government of Alberta.

The baby's mother was soon tracked down in the State of Washington. But how was Safeway able to supply that picture? I visited the store and found the inconspicuous camera posted over the entrance. Sure enough, everyone who entered was being captured on video.

Back in 2000, this was a shocking discovery for me. It seemed unnecessary for a grocery store to capture the arrival and departure of every customer on video. What else were they watching? Now, it is hard to imagine an urban space that is not within the reach of a surveillance camera. It's not just that they're capturing your image: it's what might they might do with it, now and in the future.

Just what are all those surveillance cameras doing when they are not taking pictures of suspected terrorists, shoplifters, or mothers who abandon their kids? They are watching us, creating a potentiall eternal archive of everything we do. The same technology that allows law enforcement to zoom in on bad guys can impinge on the privacy of law-abiding citizens in some very creepy ways.

The one-way nature of surveillance cameras is one of their most unsettling features. Aside from the occasional blinking light, they tell us nothing. We tell them everything. One way to level this playing field is to wear our own cameras. University of Toronto Professor Steve Mann coined the ter "sous-veillance" to describe the countermeasure of wearing cameras to record our own version of ho things happen.

One of the first famous uses of this approach was the 1991 videotaping of the beating of African-American construction worker Rodney King by the Los Angeles police. The police officers were acquitted, despite compelling video evidence against them, sparking the 1992 riots in that city.

Now, dashboard cameras are commonplace, at least in the United States, and definitely in Russia,

where they are almost mandatory to survive the country's traffic and scam artists who stage fake accidents.[46] Video evidence gives you an edge in many situations, and some people are already logging their lives as an offbeat kind of hobby. I spoke to one of these lifeloggers, and he estimates the cost of recording his every moment in audio and video at about one dollar a day for storage medi His cost in terms of relaxed social interaction, however, might be much greater. The possibility of recording everything you see, hear, smell, and touch was also the subject of a research project called Lifelog, funded by the Defense Advanced Research Projects Agency in 2003 but abruptly canceled in 2004 after privacy groups voiced objections.[47] According to many experts, the program has continue at least in spirit, both inside and outside the U.S. government.[48]

The movie *Déjà Vu* (2006) envisioned a world in which satellites look down at people and peer inside their homes with laser imaging, using computer reconstruction to replay a terrorist attack and then travel back in time to avert it. Camera technology is definitely moving in the creepy direction suggested by the movie. Scientists at MIT have announced the ability to see through solid walls to an accuracy of ten centimeters. PhD student Fadil Adib, speaking on a *Network World* video, says "we'r doing localization through a wall, without requiring you to hold any transmitter or receiver, simply b using reflections off the human body."[49]

The researchers gave their project a benign name, "Kinect of the Future," suggesting it might simply be the next evolution of Microsoft's popular gaming device. However, a system that can peer through walls will have applications far beyond video gaming. It probably would have been greeted much differently if they had called it the "Anne Frank Finder." That may indeed be much closer to how this technology will really be used.

Even before the Boston Marathon bombings, the U.S. Air Force contracted with the 3D biometric imaging firm Photon-X for a new kind of surveillance camera. By using a combination of infrared an visible light, and by indexing muscle movements that are unique to each individual, the company claims it can produce a unique "bio-signature" for a person and then silently track them.[50]

The company is also promoting something they call the Spatial Phase Imaging Technique (yielding an unfortunate acronym, SPIT), which purports to read your fingerprints at a distance of up to ten feet, with "longer distances being developed." They also claim they can "passively capture 3D geometry for skin, hair, eyes, teeth, clothing, and anything else that is in frame, with no special preparation of the subject."[51]

While surveillance cameras do not yet follow us everywhere, we do a pretty good job of filling in the gaps with our own cameras. We snap billions of photos and many of them end up on Facebook an photo-sharing websites. By putting our real name next to photos, we provide the fodder for all kinds nefarious data mining.

TV studio cameras have large red "tally lights" to show the anchorperson where to look, but far too many unwitting TV presenters have been embarrassed by their "off camera" comments that made it to air, so they don't really trust the lights.

While their lenses may be almost invisible, laptop computers and smartphones are equally risky. Unless you douse it in a glass of water, as a friend of mine did when he learned his smartphones was infected with some nasty malware, there is a decent chance that your camera can be hijacked by a hacker.[52]

Showing off clever ways to remotely invade a smartphones has been a staple of hacker conferenc for years. Now, you do not even need hacker skills to take over someone's smartphone, because "there's an app for that"—in fact, many of them. One is the notorious "Rastreador de Namorado" (Boyfriend Tracker) from Brazil.[53] Once you slip this onto someone's phone, it reports all of the