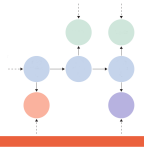


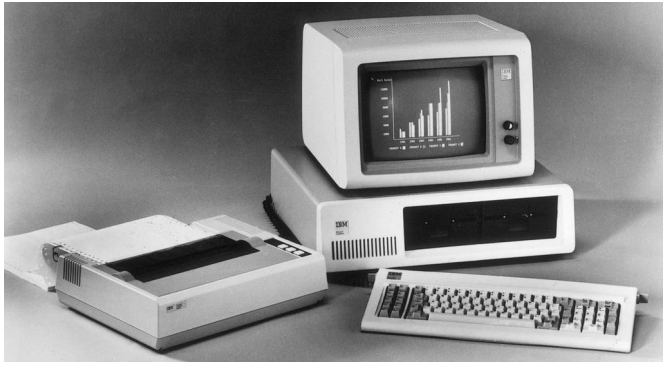
Effects, Side Effects and Risks of the Internet of Things

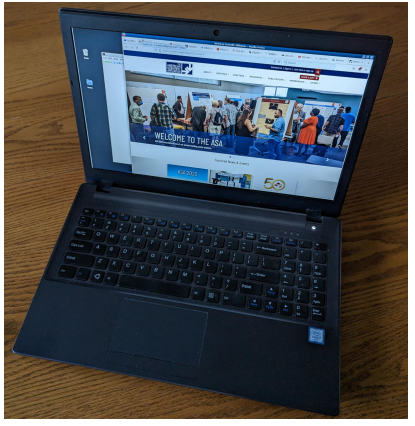
Timothy P. Wallace

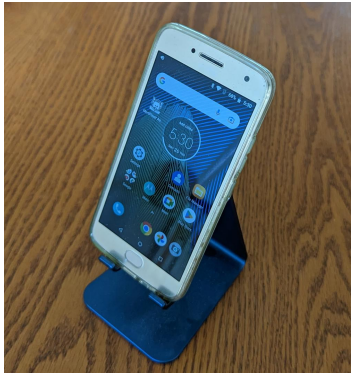
July 2023

The Evolution of Computer Products

- **The computer hardware industry promotes new, innovative products to stimulate demand**
  - **The 1980's started the PC era**
  - **Laptops took off in the 1990's**
  - **The 2007 iPhone introduction jump-started smart phones**
- **Most people who want a computer or smartphone have one at this point:**
  - **Approximately 2 billion computers are in use**
  - **Approximately 7 billion smartphones are in use**
- **As these products mature and the market becomes saturated, new products must be marketed to sustain the economic model**

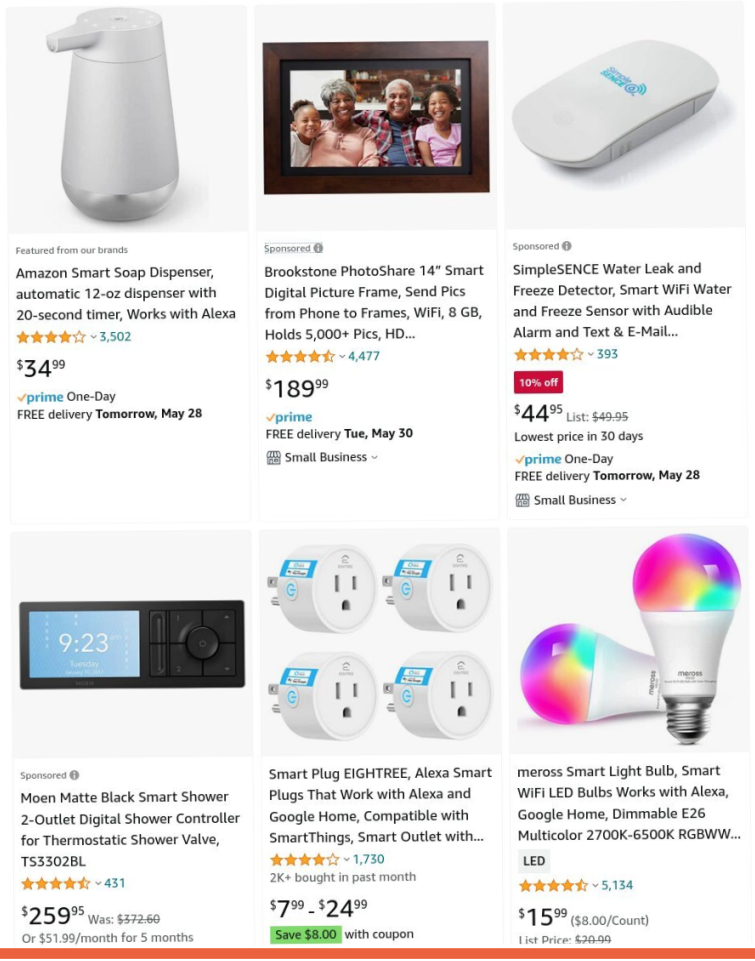






The Internet of Things (IoT)

- **The IoT puts many “smart” devices and sensors on the internet with these selling points:**
  - **You can observe and control your home devices over the internet via your computer or phone**
  - **Industry can instrument their equipment and processes to improve efficiency**
  - **Government can observe and control infrastructure with IoT devices**
- **About 10 billion IoT devices are in use today**
- **Searching Amazon for “smart” yielded the screen at right**
  - **The vast majority of “smart” products are IoT products**
  - **The IoT functionality is not always obvious!**



The Big Picture Created by the 10 Billion Small IoT Devices

- **We are putting ourselves under surveillance when we purchase and use the IoT**
- **Commercial entities are also putting us under surveillance the same way**
- **Many governments are surveilling their populations using IoT devices**
- **Hackers can cause harm by misusing IoT devices**

Amazon's Ring used to spy on customers, FTC says in privacy settlement

By Diane Bartz

May 31, 2023 11:57 PM UTC · Updated ago

WASHINGTON, May 31 (Reuters) - A former employee of Amazon.com's Ring doorbell camera unit spied for months on female customers in 2017 with cameras placed in bedrooms and bathrooms, the Federal Trade Commission said in a court filing on Wednesday when it announced a $5.8 million settlement with the company over privacy violations.

https://www.reuters.com/legal/us-ftc-sues-amazoncoms-ring-2023-05-31/

21 DEC 4 COMPANIES TO WATCH OUT FOR IN THE AUTOMATED NUMBER PLATE RECOGNITION SYSTEMS INDUSTRY

https://www.aviseanalytics.com/4-companies-to-watch-out-for-in-the-automated-number-plate-recognition-systems-industry/

Alibaba Uyghur Recognition As A Service

In 2020, IPVM reported that Alibaba openly offered Uyghur/'ethnic minority' recognition as a Cloud service, allowing customers to be alerted any time Alibaba detects a Uyghur:

At the time, Alibaba admitted its Cloud division developed the racist AI software, saying it is "dismayed" while claiming it "never intended" to target "specific ethnic groups" and the tech was only used "within a testing environment".

https://ipvm.com/reports/shanghai-police?code=soivnq080vdjij

Outline

- Introduction to the IoT (Internet of Things)
- Misuses of the IoT
- Problems When the IoT is Used as Intended
- The Christian Perspective
- Summary

Security Issues with the Internet of Things (IoT)

- The 10 billion IoT devices are rather pervasive, enabling remote observation and control
  - Security is not always foremost
  - Keeping cost low more important
  - Not all IoT software can be easily updated
- The government has IoT security standards for US Government acquisitions only
  - IoT Cybersecurity Improvement Act of 2020
  - Took effect December, 2022

Technology | DOI:10.1145/3591215

Logan Kugler

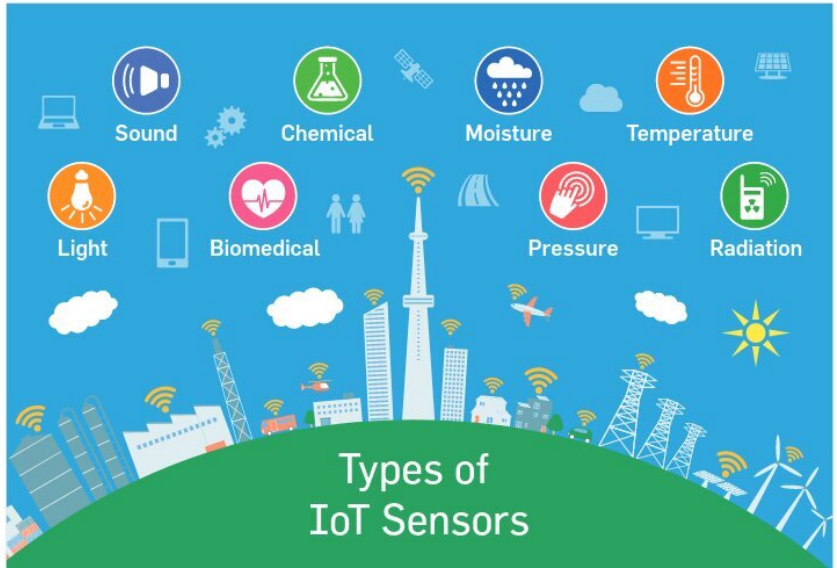
Standards to Secure the Sensors That Power IoT

Existing security standards do not always offer sufficient protection to secure the Internet of Things.

THE USE OF Internet of Things (IoT) sensors has exploded in popularity in recent years as cheap, effective IoT sensors make it possible to connect devices that do everything from regulating smart home features to monitoring health and fitness using wearable devices.

IoT sensors also are increasingly making their way into business use-cases. In the industrial IoT, sensors are used in many different contexts, including to control and monitor machinery and to regulate core infrastructure systems.

IoT device and sensor usage has accelerated even more with advances in 5G connectivity and the shift to remote work, says Willi Nelson, chief



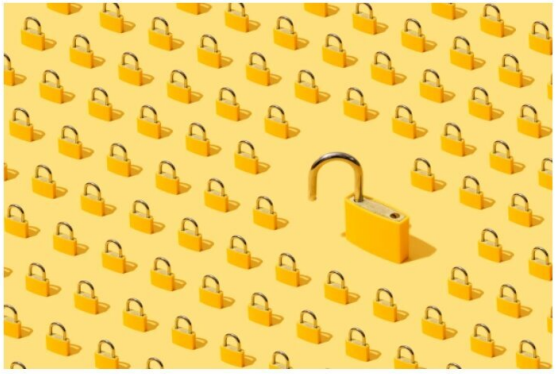
L. Kugler, Standards to Secure the Sensors that Power IoT, Communications of the ACM, Vol. 66, No. 6, June 2023, pp 14-16.

Security Issues with the Internet of Things (IoT)

- The 10 billion IoT devices are rather pervasive, enabling remote observation and control
  - Security is not always foremost
  - Keeping cost low more important
  - Not all IoT software can be easily updated
- The government has IoT security standards for US Government acquisitions only
  - IoT Cybersecurity Improvement Act of 2020
  - Took effect December, 2022

US government launches the Cyber Trust Mark, its long-awaited IoT security labeling program

Carly Page 7 days



The Biden administration has launched its long-awaited Internet of Things (IoT) cybersecurity labeling program that aims to protect Americans against the myriad security risks associated with internet-connected devices.

The program, officially named the "U.S. Cyber Trust Mark," aims to help Americans ensure they are buying internet-connected devices that include strong cybersecurity protections against cyberattacks.

https://techcrunch.com/2023/07/18/us-government-launches-the-cyber-trust-mark-its-long-awaited-iot-security-labeling-program/

Attacking a Casino Through IoT

- A famous IoT-based attack on a casino took place through their aquarium
  - An IoT aquarium thermometer connected to their local network
  - Hacking the thermometer led to other computers on the network
  - A list of high rollers and their personal and financial information was exfiltrated
- This took place in 2018, and was only revealed on condition of anonymity
- Other such events likely still happening

https://thehackernews.com/2018/04/iot-hacking-thermometer.html

#1 Trusted Cybersecurity News Platform

Casino Gets Hacked Through Its Internet-Connected Fish Tank Thermometer

Apr 16, 2018 Wang Wei

Internet-connected technology, also known as the Internet of Things (IoT), is now part of daily life, with smart assistants like Siri and Alexa to cars, watches, toasters, fridges, thermostats, lights, and the list goes on and on.

Digital Locks for Cars and Houses Not Always Secure

- Digital (IoT) locks are becoming more popular
  - Hotels using them to simplify combination change
  - Some apartments are starting to use them
  - Available for your personal residence
  - Some newer cars also use them
- There are a variety of technologies used, but many have been hacked
- The Digital Trends article at right from 2022 describes an interesting hack which applies to some IoT devices including those used in Tesla cars

Bluetooth hack compromises Teslas, digital locks, and more

By Jesse Hollington
May 16, 2022

SHARE

A group of security researchers has found a way to circumvent digital locks and other security systems that rely on the proximity of a Bluetooth fob or smartphone for authentication.

Using what's known as a "link layer relay attack," security consulting firm NCC Group was able to unlock, start, and drive vehicles and unlock and open certain residential smart locks without the Bluetooth-based key anywhere in the vicinity.

https://www.digitaltrends.com/mobile/bluetooth-hack-compromises-teslas-digital-locks-and-more/

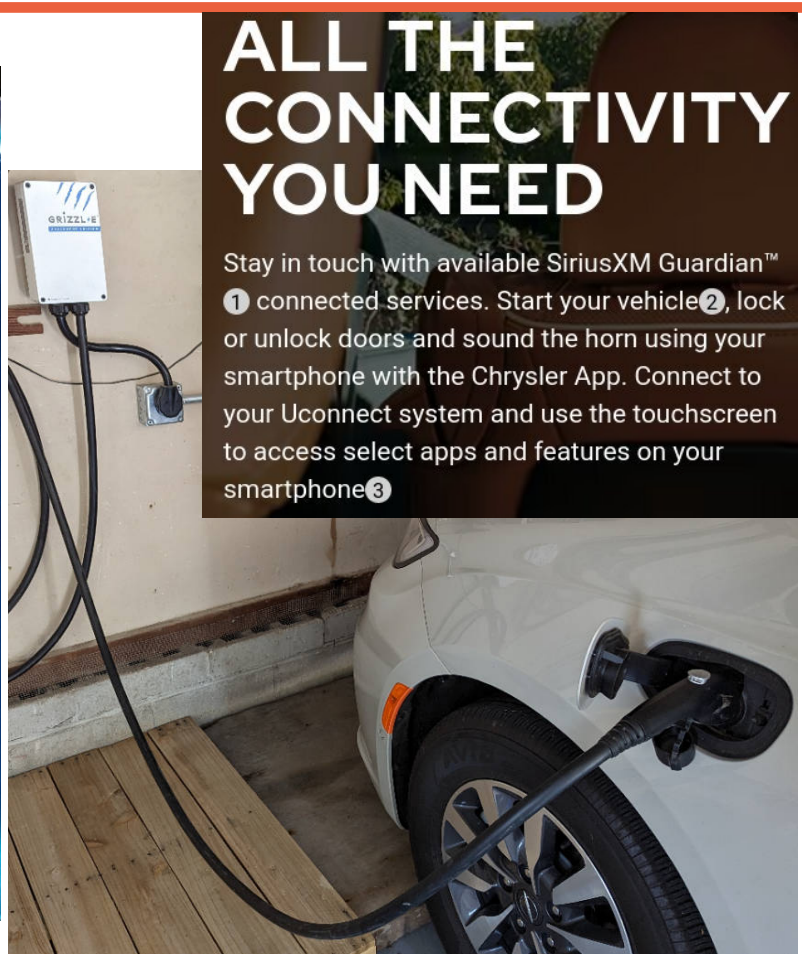
Baby Monitors Have Been Attacked for Years

- Baby Monitor hackers make for exciting stories
  - The 2023 story at right was reported by many news outlets
  - The three-year-old victim unplugged his camera to stop it!
- They've been reported for years, and now appear on TikTok
- The proper use of the devices can mitigate the threat
  - Use unique and complex password
  - Turn off remote internet access, when possible
- The panicked parents tend to just throw the devices away!

Kurin Adele (left) urged fellow parents to ditch their WiFi baby monitors after hers was "hacked" / @kurinadele/TikTok/iStock

My IoT: My Garage

- I have three potential IoT devices in my garage:
  - The opener (I saved $40 by getting non-IoT openers five years ago after my old openers were hit by lightning)
  - The Level 2 EV charger (just plug it in, and then unplug it!)
  - The Chrysler plug-in hybrid van (saved $20/month and prevented hackers from unlocking my car and/or turning it on and off)



My IoT: My Garage

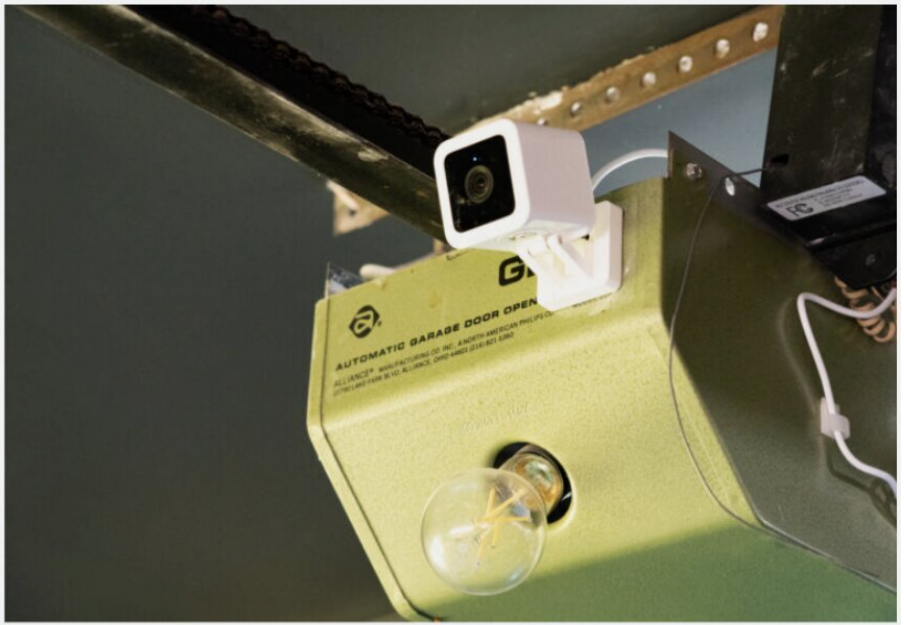
- **I have three potential IoT devices in my garage:**
  - **The opener (I saved $40 by getting non-IoT openers five years ago after my old openers were hit by lightning)**
  - **The Level 2 EV charger (just plug it in, and then unplug it!)**
  - **The Chrysler plug-in hybrid van (saved $20/month and prevented hackers from unlocking my car and/or turning it on and off)**

INTERNET OF GARAGE DOORS —

Review: Wyze's Garage Door Controller is IoT garage simplicity

An easy, secure way to make your dumb garage smart.

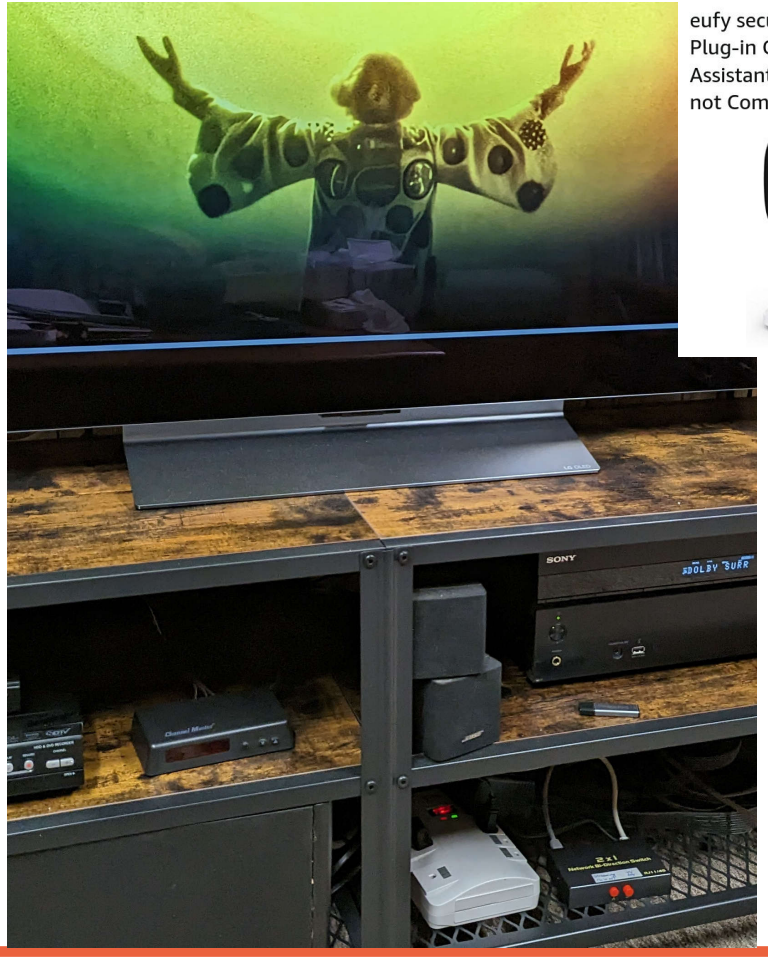
TIM STEVENS - 6/20/2023, 10:05 AM



Enlarge / Wyze's controller is a simple way to give a 50-year-old garage door opener an upgrade.

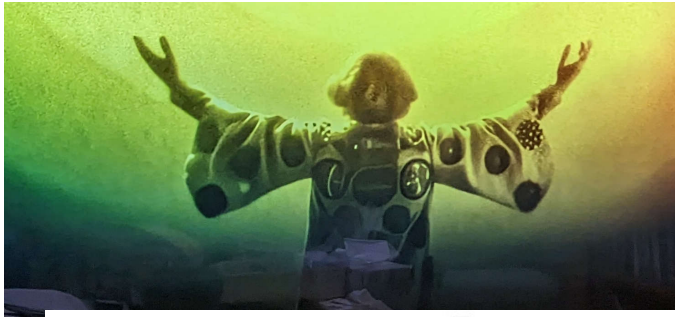
My IoT: My House

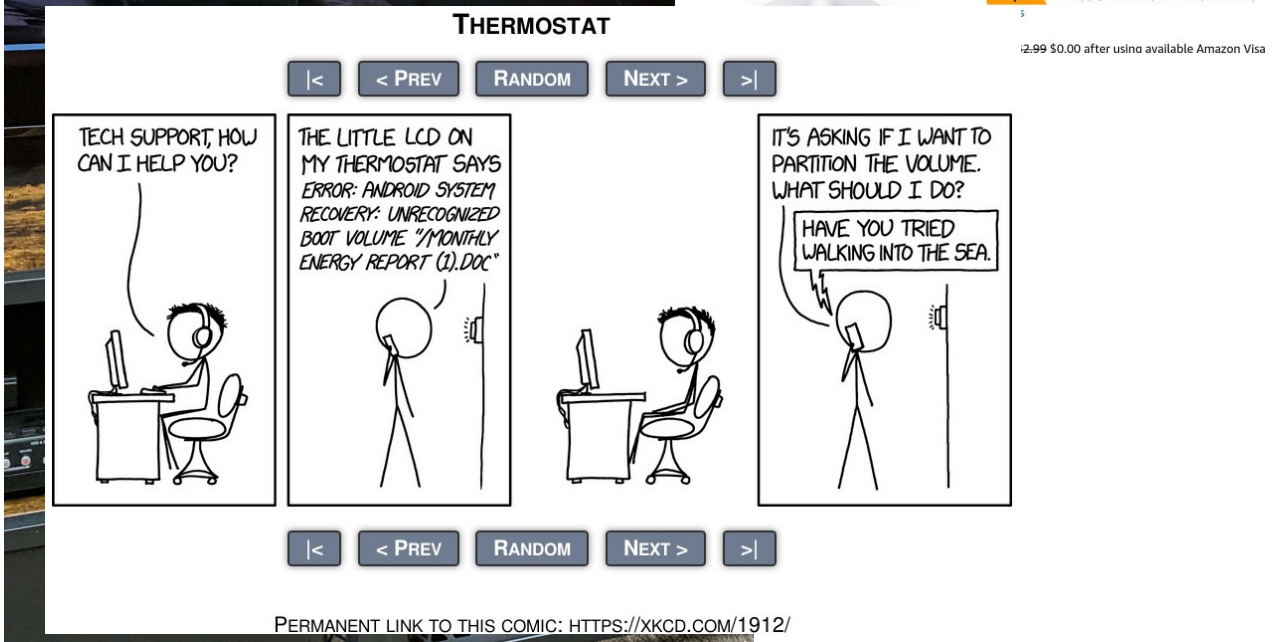
- I have IoT devices in my house
  - Smart LG TV connects to wired internet for streaming (only when switch is on!)
  - Eufy camera does not require cloud storage/control; most things done locally
- What I don't have is more notable
  - No Ring doorbell
  - No IoT digital locks
  - No IoT thermostats
  - No Amazon Echo or Alexa device



My IoT: My House

- I have IoT devices in my house
  - Smart LG TV connects to wired internet for streaming (only when switch is on!)
  - Eufy camera does not require cloud storage/control; most things done locally
- What I don't have is more notable
  - No Ring doorbell
  - No IoT digital locks
  - No IoT thermostats
  - No Amazon Echo or Alexa device





Outline

- Introduction to the IoT (Internet of Things)
- Misuses of the IoT
- Problems When the IoT is Used as Intended
- The Christian Perspective
- Summary

Google's Sidewalk Labs Project in Toronto

- **Google proposed a 12-acre "Smart City" in 2017**
  - **The Toronto site was to be heavily instrumented with IoT sensors: "ubiquitous sensing"**
  - **The goal was a more efficient city**
  - **It would record all the data and use the feedback to make the project's systems run better**
  - **This model project could be a gateway to larger projects**
  - **Proposal Illustrations were rather fanciful, and not closely connected to the reality**

The End of Sidewalk Labs

By Alex Bozikovic

Exterior of the proposed mixed-use development in Quayside. *Rendering by Picture Plane for Heatherwick Studio*

March 22, 2022

In the fall of 2017, Sidewalk Labs, a subsidiary of Google's parent company, Alphabet Inc., announced a deal in Toronto to build a dream city "from the Internet up," as CEO Daniel Doctoroff put it. The company's 220-page proposal was heavy on the physical aspects of contemporary urbanity; its colorful illustrations showed gondolas, waste-disposal robots running underground, and mixed-use modular buildings.

But the illustrations were largely whims—drawn by a junior designer at Heatherwick Studio in New York—and the actual ideas never came any closer to reality. The company had imagined a 12-acre neighborhood with an efficient energy grid and all kinds of amenities, but it also wanted to place sensors everywhere. The network of sensors would not only record useful data about energy use and occupants' behaviors, but transform this data into feedback to make the project's systems run better—what Doctoroff dubbed an "urban-tech revolution."

https://www.architecturalrecord.com/articles/15573-the-end-of-sidewalk-labs

Google's Sidewalk Labs Project in Toronto

- **In 2018, the project hit some speed bumps**
- **Privacy advocates criticized the project**
  - **Complete surveillance with many sensors**
  - **Insufficient guarantees of data limits**
  - **No guarantee of anonymization**
  - **Accusations of misinformation**
- **Some advisory board members resigned**

The Quayside site and the surrounding area. Downtown Toronto is to the upper left. (Open Street Maps / Ian Bogost / *The Atlantic*)

But all those data require mechanisms to collect them, and the march to an "always on" city has drawn an onslaught of accusations against Sidewalk Labs and its real-estate partner, Waterfront Toronto, for dismissing privacy concerns and misinforming residents. In the past month, four people have resigned from Waterfront Toronto's and Sidewalk Labs' advisory board over concerns about privacy and lack of public input.

https://www.theatlantic.com/technology/archive/2018/11/google-sidewalk-labs/575551/

Google’s Sidewalk Labs Project in Toronto

- The project was canceled in 2020
  - The pandemic was a handy excuse
  - Increasing opposition might have been a factor!
- The business case for the project was threatened
  - Pushback on data sales reduced expected revenue
  - Attempt to get tax money and payments abandoned
  - General support from public perhaps wavering
  - Canadian Civil Liberties Group sued Google

MAY 7, 2020 / 11:23 AM / UPDATED 3 YEARS AGO

Alphabet's Sidewalk Labs cancels Toronto 'smart city' project

By Moira Warburton

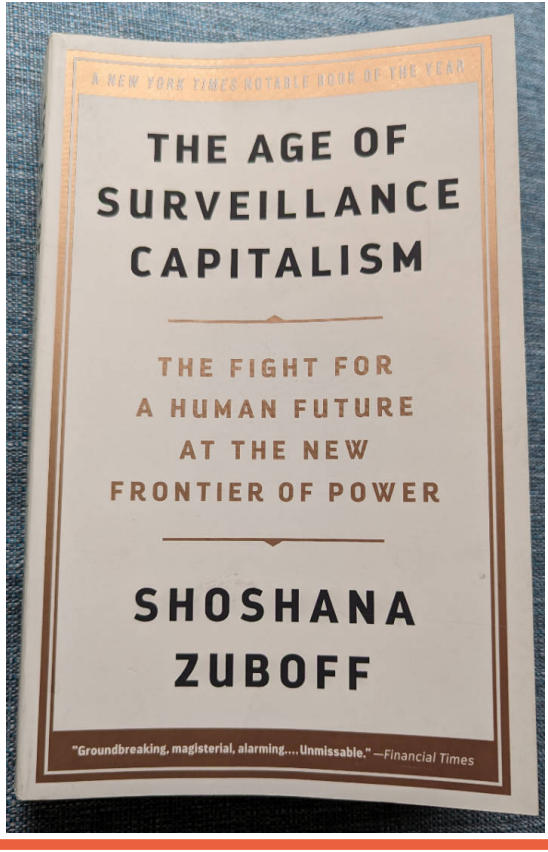
TORONTO (Reuters) - Alphabet's GOOGL.O Sidewalk Labs has pulled the plug on its Toronto "smart city" project, citing "unprecedented economic uncertainty" in a setback for the city's long-planned waterfront revitalization.

https://www.reuters.com/article/us-canada-sidewalk/alphabets-sidewalk-labs-cancels-toronto-smart-city-project-idUSKBN22J2FN

Motives of the Data Collectors: Surveillance Capitalism

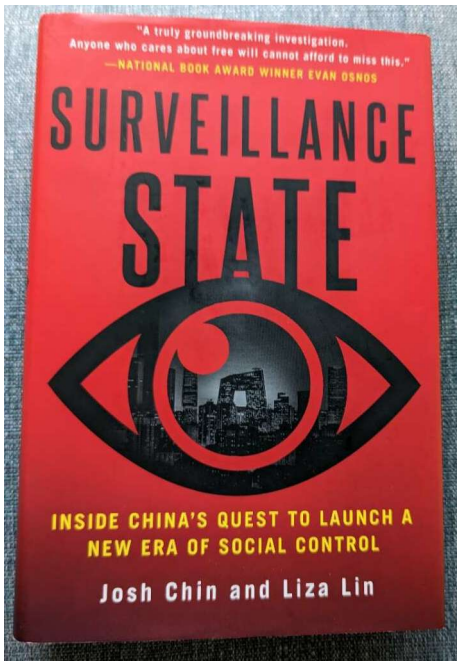
- **Surveillance capitalism unilaterally claims human experience as free raw material for translation into behavioral data. Although some of these data are applied to product or service improvement, the rest are declared as a proprietary *behavioral surplus*, fed into advanced manufacturing processes known as "machine intelligence," and fabricated into *prediction products* that anticipate what you will do now, soon, and later.**

- **A senior systems architect: "The IoT is inevitable like getting to the Pacific Ocean was inevitable. It's manifest destiny. Ninety-eight percent of the things in the world are not connected. So we're gonna connect them. It could be a moisture sensor that sits in the ground. It could be your liver. That's *your* IoT. The next step is what we do with the data. We'll visualize it, make sense of it, and monetize it. That's *our* IoT.**



Totalitarian Government Use of the IoT

- Totalitarian governments are notorious for surveillance
  - Political opponents and disfavored organizations often targeted
  - Potential separatist regions or peoples get special attention
- China is the largest and richest totalitarian government
  - They have targeted the domestic Falun Gong movement
  - Foreign NGOs and religious groups have come under pressure
  - Treatment of the Uyghurs in the Xinjiang region has been called genocide
- By no means is China the only offender
  - More democratic countries are also using pervasive surveillance
  - China will sell anyone some nice hardware and software packages



Shanghai Police Track Uyghurs and Journalists Visiting Xinjiang

- **The IoT generates a lot of data**
  - **Most IoT devices cannot process the data**
  - **Fusion of data from multiple sites needs central location, anyway**
  - **The “cloud” processes the data**
- **This article from the IPVM web site describes surveillance**
  - **Cameras feed data to the cloud**
  - **Journalists (individually) and Uyghurs (as a race) are identified**
  - **Pervasive cameras enable tracking of these people in Xinjiang or Shanghai**

Shanghai police are building a sweeping surveillance system which notifies authorities whenever foreign journalists book flights or train tickets to Xinjiang.

The system also flags police whenever a Uyghur arrives in Shanghai. All this is made possible by connecting directly to Shanghai's Alibaba police cloud.

The PRC is accused of perpetrating "serious human rights violations" in Xinjiang by the UN. Foreign journalists traveling to Xinjiang report being followed, harassed, and even assaulted.

Alibaba did not respond to repeated requests for comment. (Alibaba previously offered Uyghur recognition as a service but claimed it was for 'testing'.)

In this post, IPVM examines this project and the risks it raises. *National Review* has covered this report.

https://ipvm.com/reports/shanghai-police?code=soivnq080vdjij

Shanghai Police Track Uyghurs and Journalists Visiting Xinjiang

- **Here is an actual screen capture of the surveillance software**
- **The instructions are helpfully in both English and Chinese**
- **This module flags foreign journalists with an interest in Xinjiang**

Flags Foreign Journalists Traveling To Xinjiang

One of the 26 'modules', the "Special Personnel Screening Mode" (特因人员梳理模型), creates a system that automatically flags foreign journalists with travel records to Xinjiang, either by plane or by train:

IPVM

8	Special Personnel Screening Mode	**Filter flight or train records that have been to Xinjiang** and cross-check that with the basic information of the overseas personnel database to extract the information of personnel that has been to Xinjiang, and relate that to the information of **foreign journalists living in China** as well as the information of real personnel that have changed their ID in Shanghai to generate information on overseas personnel special groups.
8	特因人员梳理模型	筛选去过新疆等地的民航或火车出行信息，并对比境外人口基本信息表取出去过新疆人员信息，并关联外国驻华记者信息，在沪变换身份信息的实有人口信息，生成境外人员特殊群体信息

Xinjiang is ~2,500 miles from Shanghai so virtually all journalists wishing to go there book an airline ticket or at least a high-speed train.

https://ipvm.com/reports/shanghai-police?code=soivnq080vdjij

Shanghai Police Track Uyghurs and Journalists Visiting Xinjiang

- **This module locates Uyghurs who are subject to special scrutiny when they leave Xinjiang**
- **Police interrogations are very common and can happen at any time**

"Spot Uyghurs Coming To Shanghai"

Another one of the 26 modules creates a system that can automatically "spot Uyghurs coming to Shanghai":

IPVM

2	Verification Feature for Historical Addresses of Uyghurs Coming to Shanghai	**Spot Uyghurs coming to Shanghai**, verify their historical addresses through the real personnel database.
2	来沪维族人员历史地址核查功能	发现来沪维族人员，通过实有人口库、核查历史地址

While the exact purpose of this 'module' is unclear, Uyghurs are subject to "heightened monitoring and control" when they travel within China and are often interrogated by police as soon as their presence is known, Human Rights Watch told IPVM:

https://ipvm.com/reports/shanghai-police?code=soivnq080vdjij

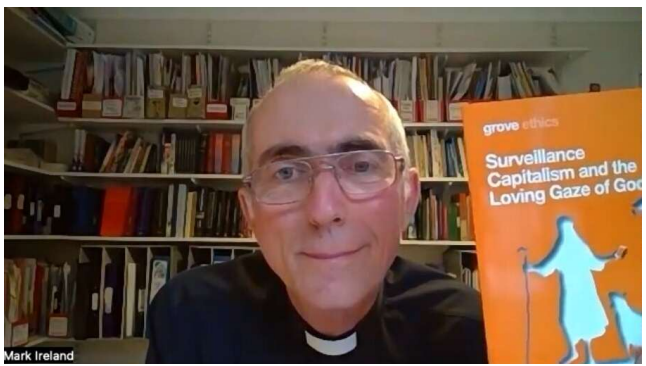
Outline

- Introduction to the IoT (Internet of Things)
- Misuses of the IoT
- Problems When the IoT is Used as Intended
- The Christian Perspective
- Summary

The Biblical View of Surveillance

- **Traditionally people talk about the "loving gaze of God."**
  - **Unless the LORD watches over the city, the guards stand watch in vain. (Psalm 127:1, NIV)**
  - **"You are the God who sees me," for she said, "I have now seen the One who sees me." (Genesis 16:13, NIV, Hagar speaking)**
  - **For the eyes of the LORD run to and fro throughout the whole earth, to give strong support to those whose heart is blameless toward him. (II Chronicles 16:9, ESV)**

- **Surveillance on earth is all about the motives**
  - **Christian response to Surveillance Capitalism: Mark Ireland**
  - **Eric Stoddart, *The Common Gaze: Surveillance and the Common Good***
  - **Surveillance that exploits the vulnerable should be avoided**
  - **Most Christians know which motives are problematic**



https://www.youtube.com/watch?v=G30EAX5dQWc

Summary of Five Talks

- This is my fifth talk on issues raised by digital technology
  - 2018 AI: Artificial stupidity and misuse of over-marketed “AI” is the real problem
  - 2019 Cyber: Hubris and capitalism have created highly insecure infrastructure we all use
  - 2021 Social media: Companies monetizing our attention creating serious social problems
  - 2022 Bias in AI: Algorithms marketed as saving money while reducing bias more likely to increase it
- The IoT sounds like the first hardware talk, but the real issue is the data collected:
  - The surveillance power largely rests with the corporations in the West

    Our legal strictures are aimed at government rather than private industry
  - The surveillance power rests with the government in autocratic regimes
- Digital technology is having tremendous effects and side-effects here and world-wide
- I believe that ASA should continue to discuss these issues