Internet of Things: Gaslighting and the Smart Home

Introduction

The "Internet of Things" is poised to shape societies for years to come. The vision is for physical objects, of all kinds in all places, to dynamically and intelligently respond to human needs and circumstances. Manufacturers and tech optimists promise more efficiency and happiness. The *New York Times* puts it this way:

> Cars, door locks, contact lenses, clothes, toasters, refrigerators, industrial robots, fish tanks, sex toys, light bulbs, toothbrushes, motorcycle helmets — these and other everyday objects are all on the menu for getting "smart." Hundreds of small start-ups are taking part in this trend — known by the marketing catchphrase "the internet of things" — but like everything else in tech, the movement is led by giants, among them Amazon, Apple and Samsung.

The constellation of technologies that make up the Internet of Things will, in all likelihood, create benefits and lead to new social and economic opportunities. On the other hand, just as likely, the Internet of Things will also enable inappropriate or unsafe behaviors, create challenges and unintended consequences, and lead to harms.

According to Melvin Kranzberg, a philosopher of technology, any "technology is neither good nor bad; nor is it neutral." Accordingly, the Internet of Things will surely be empowering and problematic at the same time, a double-edged sword. How empowering? How problematic? And, for whom? While somewhat difficult to predict, the social and economic impacts of this foundational technology, experienced directly and as ripple effects, are likely to be very substantial. At least the following values are at stake: privacy, security, control, and freedom.

Leading technologists, Francine Berman and Vinton Cerf, write: "The difference between an IoT [Internet of Things] that enhances society and one that diminishes it will be determined by our ability to create an effective model for IoT governance" (Berman & Cerf, 2017). One approach for discovering what a model of governance needs to address is to explore worse-case scenarios—that is, what might go wrong and what might be done so that big problems are less likely to occur.

Stepping back, the Internet of Things can be viewed as a network of objects and devices that compute, sense, exchange information, and respond. With some engineering, anything that has an on-off switch might plausibly become part of the Internet of Things. By 2020, it is expected that more than 30 billion things will be connected to the Internet. More impressive still, the Internet of Things is a unifying technology because a smart object might be located anywhere: in cyberspace, in the built environment, and in biological systems. Even ordinary things such as paint, food, and, indeed, potentially, in any material, might be made smart in the future.

The "Smart City," for example, refers to a vision of greater efficiency, safety, and less environmental impact. Sensors embedded in roads might monitor traffic volumes and dynamically adjust highway tolls, optimizing traffic flows, based on the willingness of people to pay for fast travel times. Safety cameras, mounted on traffic lights, might be used to enforce the rules of the road. Automatic license plate readers might identify drivers, or at least cars, who are speeding or running red lights. This technology, however, might collect and store data on the movement of people which, in turn, might be useful for identifying welfare fraud and other crimes. In so doing it might also violate individuals'

privacy. On-board sensors in buses might monitor locations and expected arrival times at bus stops, and send updates to mobile phones. In the Smart City many different data streams might be brought together to offer an overall model of the city and reveal patterns of where groups and individuals go.

The "Smart Store," such as Amazon Go, eliminates check-out lines. Enter the store, identify yourself by scanning a mobile phone at a turnstile, shop as you normally would, and just leave the store—voila, no lines, a more efficient shopping experience, and individual empowerment. Perhaps facial recognition technology or ID chips embedded in customers' bodies will do away with the need to explicitly authenticate with a phone. It has been reported that Amazon is going to open 3,000 such stores by 2021, targeting neighborhoods of affluent, young urbanites. People with low incomes, or those who decide against owning a mobile phone or object to using a phone to authenticate in pubic spaces, are unlikely to use Smart Stores. Similarly, cars might be equipped with communication capabilities for purchasing products and services. While out and about, order your favorite coffee drink, pick it up at the nearest drive-thru, and use your shopping cart to pay for it—easier, more efficient transactions, and perhaps more control on how one's time is spent.

The "Smart Home" promises greater control, efficiency, and safety, for new and better human experiences at home. In the Smart Home, lightbulbs, door bells, furnaces, lights, air conditioners, coffee pots, and locks will be controlled from a mobile phone. Offering pleasure and efficiency, smart speakers, which translate the human voice and language into commands for the Internet of Things, might become the control center of homes. But, such speakers, unbeknownst to people at home, might also be able to identify highly personal things such as indicators of mental illness. Toys and vacuum cleaners, connected to the Internet, might respond to human commands and home conditions. Hidden cameras, sometimes called "nanny cams," might be used to monitor the front door or the baby's room. Other home cameras, installed in the living room and kitchen, might be used by adult children to keep in touch with their elderly parents. Sensors in the floors might identify when an elder falls or when their balance is deteriorating or improving after, for example, a hip replacement. The same sensors might also learn to identify people by their gait and detect familiar and first-time visitors. Smart meters measuring electricity and water consumption might enable homeowners to save money and reduce their home's environmental impact. However, should a third party gain access to time-series data of electricity and water consumption a good deal might be inferable, for example, television watching, cooking, and showering habits.

The "Smart Body," might contain sensors that measure vital indicators of health, enabling people to set goals, measure progress, and keep medical personnel appraised. Such data might restructure the doctor-patient relationship and make it more patient-centered. With granular analysis of sensor data in combination with atmospheric data—temperature, pollen counts, measures of particulate concentrations—new discoveries in health care might be made. At the same time, life insurance companies might use this data to dynamically adjust their rates. In a different vein, police departments might use data about individuals—their location, sleeping patterns, and physiological measures—to help solve crimes.

The Internet of Things on a "Smart Farm" might signal such information as: It's time to irrigate the corn (because a sensor indicates that the soil is dry), it rained 5 mm yesterday, a predator threatens the herd of cattle (because the heard is sending a collective signal of anxiety), the feed stock is low, the cold storage room is up to 3 Celsius, someone is in the barn, the gate was left open.

In wild places, the "Smart Ecosystem," might be designed to include sensors and cameras, strategically placed in the woods, for investigating the movements of wildlife. When chips are embedded in wolves and livestock, for example, wildlife managers might monitor their travels and, like a video game, zap them with an electric shock to keep them separated. No plausible? Perhaps. But, with the Internet of things, if it can be imagined, it might be possible. Perhaps, via their mobile phones, hikers will be informed of the presence of a nearby grizzle bear. But, what of hunters: Should they be informed?

As these examples show, the opportunities to deploy the Internet of Things appear to be boundless, limited only by our technical imagination for new human experiences. Yet, in these examples, we can also discern the double-edged sword of this technology, where features and capabilities might produce benefits, along with harms and potentially distressing consequences.

One stunning example of a harm occurred on October 21, 2016 when the Internet of Things was exploited to execute a distributed denial of service attack, the so-called "2016 Dyn cyberattack." It is believed that the attackers constructed a botnet by infecting residential printers, cameras, baby monitors, and so forth with malware. That malware was used to flood an Internet domain name service with so many requests that legitimate requests could not be served, leading to major websites being unavailable. The root cause of the attack was poor security of ordinary residential objects that were connected to the Internet. In another example, in May 25, 2018 the FBI issued a public service announcement, requesting all owners of small office and home routers to reboot them. Bad actors had introduced malware that could be used to exploit routers and to capture information and render them inoperative.

Design Activity

Design Groups

Please divide into groups of four and proceed through this design process.

Design Setting

Note: This scenario contains potentially distressing content related to domestic abuse.

Consider the Internet of Things in the context of an affluent home, that is, a home where its occupants have sufficient discretionary income to purchase the latest Internet-ready devices. Take a worst-case scenario:

Value Scenario: Smart Home or Haunted House

Sally and Bill once lived together in a smart home in an affluent neighborhood. They are now separated because of Bill's controlling and abusive behavior. Sally continues to live in their once happy home; Bill lives in an apartment several miles away.

In their home dozens of everyday objects are connected to the Internet of Things – cameras, locks, air conditioners, thermostats, televisions and media players, alarm clocks, lighting controls, floor sensors, and so forth. Bill knows the home network well, the passwords, how to control the security cameras, how to access data, and so forth. Sally, however, has less knowledge.

In anger and for revenge, Bill cruelly manipulates and diabolically fiddles with the smart objects of their home, causing Sally to question her memory, perception, and, in time, her sanity. The smart home is the perfect technology for control and abuse, for creating a "haunted house" or for "gaslighting."

First described by British psychiatrists in 1969, the term gaslighting comes from a stage play, Gaslight, where a husband surreptitiously manipulates small elements at home, including the lighting, light provided by gas, seeking to induce insanity in his wife.

Design Prompt

A product team working on smart devices for domestic settings seeks to prevent their technologies from being used for domestic abuse. What technical features and policy elements should be built into their socio-technical systems?

A Simplified Value Sensitive Design Process

(1) *Identify the direct and indirect stakeholders*
Direct stakeholders are, basically, users. Indirect stakeholders are impacted by a technology but do not interact with it. Stakeholders have roles and can be people, institutions, non-human animals, and, in general, any entity with moral standing. Please see methods hand-out.

(2) *Identify the values and the value sources*
In value sensitive design, a human value is defined as "what is important to people in their lives, with a focus on ethics and morality." Values are held by stakeholders or by designers. Explicitly supported values guide the design process. Please see methods handout.

(3) *Identify harms and benefits*
Related to values, explore the possible harms and benefits that the stakeholders might experience. Select several stakeholders. Then, identify the possible harms and benefits that each stakeholder might experience.

(4) *Identify value tensions*
Also related to values, are value tensions. A value tension arises when two values somehow lead in different directions. For example, a classic tension seems to exist between "physical security" and "privacy," that is, by being monitored (giving up privacy) a person can obtain physical security. Or, as young teenagers seek "independence" from their parents they may give up aspects of their "safety." Here, the values are "physical security," "privacy," "independence," and "safety" are connected into a web with some tensions.

(5) *Co-evolution of technology and social structure: Identify relevant policy elements*
Policy elements, which expand the technical design space, might include: Usage guidelines, training certifications, rules, regulations, laws. Value sensitive design makes a commitment to an *interactional stance*, where, simply put, stakeholders are assumed shape the design and use of technology and, in turn, technologies shape stakeholders and society. Please see methods handout.

(6) *Revise the value scenario*
Given your design work (steps 1-3), write a new value scenario that shows how IoT in the home can be designed such that domestic abuse is less likely to occur and in the unfortunate event it does occur institutions and society are positioned to meaningfully respond. Please see methods handout.

Studio reporting and presentation

Concept map
Consider your design work for the first four steps. How might it all be brought together into a single working model. Develop a concept map showing stakeholders, values, and value tensions. Seek to include as much detail as possible. Please see methods handout.

Poster presentation
Develop a poster and a 1-minute presentation. In your presentation, please (1) State the goal of your work and why it matters; (2) Give and overview of your process; and (3) Highlight a couple of key findings of your work which will be present in the concept map. Select a single person to present.

Reflections about your design work: Discussion questions

1. In general, how did the process go? Did you encounter any challenges? How did you overcome them? What steps were the most helpful?
2. How did you use the sticky notes in your design work? What worked? What would you do differently next time?
3. What kind of stakeholders did you identify? Did you identify any non-human stakeholders, government agencies, technical stakeholders? Did you rule out the consideration of any stakeholders? On what basis did you do that?
4. What questions do you have about stakeholder analyses? What worked well? What would you do differently next time?
5. What kind of policy elements did you employ in your design?
6. Were there aspects of the design situation that you did not cover?

DELIVERABLE: Design Activity: D01: Stakeholders Analysis / Value Scenario

Due: Friday, April 19, 3:00 PM (Two studios are devoted to this Design Activity)

For this deliverable, your goal is to write a report comprising the following sections. *Note*: Please use the report template on the course website, and please use the section headings as outlined below.

Note: Please complete this deliverable in groups of four.

Section Heading	Purpose
Title, authors, keywords and abstract	Give your report a descriptive title, include your names, include a list of 3-5 key words, and include a 100-120 word abstract.
Introduction	Briefly summarize the problem (About ½ page.)
Process	In your own words, briefly summarize the VSD process that you followed in a table or some appropriate list. Include a **photograph** or sequence of photographs of your studio team working. (One page or less.)
Concept Map	Present your concept map and include a **detailed caption** that tells the reader what to pay attention too. Seek to show a lot of detail (high information density) but also aim for clarity and, indeed, beauty. (One page or less.)
Stakeholder Analysis	Present a **comprehensive list** – as a table or diagram – of the stakeholders. Select three stakeholders for greater analysis and description. Explain why you chose those stakeholders (One page or less.)
Values and value tensions	With your list of values, create a diagram that shows how the values might be related to each other. Provide **working definitions** of three of the values. Briefly discuss how the values might be related. Are there tensions, conflicts, or trade-offs among the values? (One page or less.)
Value Scenarios	Present your value scenario (be sure it has a title). Include a brief description on what it represents.
Discussion	Summarize your views on smart homes and how they might be designed to avoid domestic abuse situations. Discussion, especially, how policy and technical elements were brought into the design space (One page or less.)
Conclusion	Wrap up the report with a brief summary and key takeaway (Less than ½ page.)
Appendix A: Reflections on Design Process	Take up one or more questions in the Studio Reflections on Design and critically reflect on your design process. (One page or less)
Appendix*	If you really need to include more material please put it into one or more appendices.

Format and grading. Please use the report format found on the course website. Your report will be graded against the following general criteria:

(1) *Overall*. All of the sections are present in the report. The writing is concise, interesting, and free of spelling and grammatical errors. You use the report template appropriately, employing good style and respecting the format. If necessary you go beyond the format elegantly and appropriately. All figures and tables have concise and clear captions. The title of the report is interesting and does not include "INFO-444" or "D01."

(2) *Process*. You concisely document the process – framing it as a VSD process. The photograph(s) clarify the tone and focus of your work.

(3) *Concept map*. The concept map is detailed and clear. It shows the direct and indirect stakeholders, values, value tensions, and other useful information about the design situation. The concept map has a concise and detailed caption.

(4) *Stakeholders*. You present a comprehensive list and clarify the details of three stakeholders. You provide working definitions for some of the values discuss 1-3 potential value tensions.

(5) *Value scenarios*. The scenarios clarify the design situation and linked to the concept map. The scenarios are written according to the envisioning criteria.

(6) *Discussion*. The discussion is concise, clear, and convincing. You take a critical stance and present a reasonable and strong path forward.

(7) Reflections. The reflections are focused and critical.

(8) *Other*. All the report components are present. The writing is concise, clear, and interesting. The report is free of spelling and grammatical errors. The material is formatted clearly and professionally.

Notes and further reading

Introduction

1. The *New York Times* quotation comes from Manjoo (2018).
2. For an introduction to the Internet of Things see FTC Staff Report (2015).
3. For a short discussion of the possible benefits of IT Governance, see Berman & Cerf (2017).
4. The number of expected objects in the Internet of Things comes from Statista (n.d.).
5. Stenquist (2018) describes cars with communication functions that simplify purchasing things and services, saving people time.
6. Data collected from automatic license plate readers have been used to identify welfare fraud and for other such purposes but at the cost of individual privacy and perhaps in ways that violate law (Maass, 2018; Fussel, 2018).
7. Soper (2018) provides a brief introduction to Amazon Go. See also González (2016).
8. The reported number of new Amazon Go stores comes from Super (2018).
9. On the use of facial recognition technology to improve efficiency in lines, see Alan (2018).
10. Cook (2018) reports on a patent awarded to Amazon that identifies illness based on the qualities and affect of a speaker's voice.
11. Hauser, C. (2018) reports on the police using Fitbit data as evidence for identifying and charging a murderer.
12. The questions that might be answered at a "Smart Farm" comes from Sigfox. (n.d.).
13. For IBM's public service announcement related to home routers, see FBI (2018).
14. For more on the 2016 Dyn Cyberattack, see 2016 Dyn Cyberattack - Wikipedia (n.d.).
15. For more on Internet of Things botnet threats, see Weagle (2018).

Design Setting

1. The New York Times reports that smart homes are being used in domestic abuse cases (Bowles, 2018).
2. Gaslighting was first described by Barton & Whitehead (1969). See also Cawthra, O'Brien, & Hassanyeh (1987).

References

2016 Dyn cyberattack - Wikipedia. (n.d.). Retrieved October 7, 2018, from https://en.wikipedia.org/wiki/2016_Dyn_cyberattack

FTC Staff Report (2015). *Internet of Things: Privacy & Security in a Connected World*. Retrieved October 16, 2018, from https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

Alan, L. (2018, October 15). TSA bringing facial recognition to airport security lanes | The Seattle Times. Retrieved October 16, 2018, from https://www.seattletimes.com/business/tsa-bringing-facial-recognition-to-airport-security-lanes/

Barton, R., & Whitehead, J. A. (1969). The Gas-Light Phenomenon. *The Lancet*, *1*, 1258–1266.

Berman, F. And Cerf, V. G. (2017). Social and ethical behavior in the Internet of Things. *Communications of the ACM*, *60*(2), 6-7.

Bowles, N. (2018, June 23). Thermostats, Locks and Lights: Digital Tools of Domestic Abuse - The New York Times. Retrieved October 17, 2018, from https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html

Cawthra, R., O'Brien, G., & Hassanyeh, F. (1987). 'Imposed Psychosis': A Case Variant of the Gaslight Phenomenon. *British Journal of Psychiatry*, *150*(4), 553-556. doi:10.1192/bjp.150.4.553

Cook, J. (2018, October 9). Amazon patents new Alexa feature that knows when you're ill and offers you medicine. Retrieved October 12, 2018, from https://www.telegraph.co.uk/technology/2018/10/09/amazon-patents-new-alexa-feature-knows-offers-medicine/

FBI. (2018, May 25). Internet Crime Complaint Center (IC3) | Foreign Cyber Actors Target Home and Office Routers and Networked Devices Worldwide [Public Service Announcement]. Retrieved October 11, 2018, from https://www.ic3.gov/media/2018/180525.aspx

Fussel, S. (2018, October 16). In Fraud Detection, Everything You Do Online and Off Is a Clue. *The Atlantic*. Retrieved from https://www.theatlantic.com/technology/archive/2018/10/online-fraud-detection-surveillance/573175/

González, Á. (2016, December 5). Amazon unveils smart convenience store sans checkouts, cashiers | The Seattle Times. Retrieved from https://www.seattletimes.com/business/amazon/amazoncom-unveils-self-driving-brick-and-mortar-convenience-store/

Hauser, C. (2018, October 3). Police Use Fitbit Data to Charge 90-Year-Old Man in Stepdaughter's Killing - The New York Times. Retrieved October 7, 2018, from https://www.nytimes.com/2018/10/03/us/fitbit-murder-arrest.html

Kranzberg, M. (1986). Kranzberg's laws. *Technology and Culture*, *27*, 544-560.

Maass, D. (2018, July 31). County Welfare Office Violated Accountability Rules While Surveilling Benefits Recipients | Electronic Frontier Foundation. Retrieved October 17, 2018, from https://www.eff.org/deeplinks/2018/07/county-welfare-office-violated-accountability-rules-while-surveilling-benefits

Manjoo, F. (2018, October 10). A Future Where Everything Becomes a Computer Is as Creepy as You Feared - The New York Times. Retrieved October 11, 2018, from https://www.nytimes.com/2018/10/10/technology/future-internet-of-things.html

Sigfox. (n.d.). Retrieved October 17, 2018, from https://www.sigfox.com/en/agriculture

Soper, S. (2018, September 19). Amazon Said to Plan Up to 3,000 Cashierless Stores by 2021 - Bloomberg. Retrieved October 7, 2018, from https://www.bloomberg.com/news/articles/2018-09-19/amazon-is-said-to-plan-up-to-3-000-cashierless-stores-by-2021

Statista. (n.d.). IoT: number of connected devices worldwide 2012-2025. Retrieved October 4, 2018, from https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

Stenquist, P. (2018, October 14). Order a coffee and pay, with a tap on your car's dash | The Seattle Times. Retrieved October 16, 2018, from https://www.seattletimes.com/business/order-a-coffee-and-pay-with-a-tap-on-your-cars-dash/

Tarnoff, B. (2018, August 9). Can Silicon Valley workers rein in Big Tech from within? | Ben Tarnoff | Opinion | The Guardian. Retrieved October 15, 2018, from https://www.theguardian.com/commentisfree/2018/aug/09/silicon-valley-tech-workers-labor-activism

Weagle, S. (2018, January 30). The Rise of IoT Botnet Threat and DDoS attacks | Corero. Retrieved October 17, 2018, from https://www.corero.com/blog/870-the-rise-of-iot-botnet-threats-and-ddos-attacks.html