Countermeasures: Learning to Lie to Objects

Angus Main
Royal College of Art
London, UK
angus.main@rca.ac.uk

ABSTRACT

Ubiquitous computing is leading to ubiquitous sensing. Sensor components such as motion, proximity, and biometric sensors are increasingly common features in everyday objects. However, the presence and full capabilities of these components are often not clear to users. Sensor-enhanced objects have the ability to perceive without being perceived. This reduces the ability of users to control how and when they are being sensed. To address this imbalance, this project identifies the need to be able to deceive 'smart' objects, and proposes a number of practical interventions to increase user awareness of sensors, and encourage agency over digital sensing through acts of dishonesty to objects.

KEYWORDS

Sensors; Internet of Things; Ubiquitous Computing; Privacy; Deception

ACM Reference Format

Angus Main. 2019. Countermeasures: Learning to Lie to Objects. In *CHI Conference on Human Factors in Computing Systems Extended Abstracts (CHI'19 Extended Abstracts), May 4–9, 2019, Glasgow, Scotland, UK.* ACM, NY, NY, USA. 10 pages. https://doi.org/10.1145/3290607.3310420

CHI'19 Extended Abstracts, May 4-9, 2019, Glasgow, Scotland, UK.

ACM ISBN 978-1-4503-5971-9/19/05...$15.00 https://doi.org/10.1145/3290607.3310420

1 CONTEXT

Sensor components are found in increasing quantity across a broad range of common 'smart' devices, such as phones, wearables, and domestic appliances. The commercial growth of this type of product means that what in the past may have been regarded as 'dumb' objects, such as door handles [29], shoes [2], or toasters [11], now have the potential to perceive and communicate.

Whatever the ultimate utility of these products, the increased presence of sensors in everyday objects raises issues of agency, privacy and consent for users, and provokes a re-evaluation of the relationship between people and the objects that surround them.

Unlike manual input mechanisms, sensors do not require attentive and deliberate use of an interface, but can instead actively and persistently observe physical attributes of a user or environment. The result of this is that users may not always be aware of the extent of their interaction with an object or the digital system it represents.

As events such as the Facebook Cambridge Analytica breech [8] make the users of online digital systems increasingly aware of issues relating to the data they are generating and sharing, there is a risk that physical sensor technology represents something of a blind spot. Online interfaces already offer some accessible tools to enable users to control or manipulate the information shared with online systems, for example "Incognito Mode" [10] and Ad Blockers for web browsers [1], or consumer-level VPN (Virtual Private Network) services. However, there is a lack of equivalent functionality for object-based systems. Whilst the motivations for lying as a privacy-protective behaviour [24] might be similar in virtual and physical environments, the means of deception are significantly different.

2 LYING TO OBJECTS

2.1 Technical dishonesty

Browser-based privacy tools such as those mentioned above represent a form of low-level, semi-sanctioned deception of online systems by users. Their availability indicates two important qualities amongst users: awareness and agency. The fact that there is popular demand for browser features that limit or obscure online activities demonstrates that users have an awareness that their behaviours are potentially subject to observations outside of their immediate context. Mindful of this, they seek access to tools which give them a degree of agency over the observations being made. This agency takes the form of a wilful non-compliance – rejecting the expected information exchanges. These acts of technical dishonesty allow the user to regain some control over their information.

Figure 1: ***I Spy Sensors*****, cover page. A guidebook to sensors that forms the first part of the Countermeasures project. © Angus Main**

This project aims to take the prerequisite conditions of that dishonesty – awareness followed by agency – and apply it to interactions with physical objects.

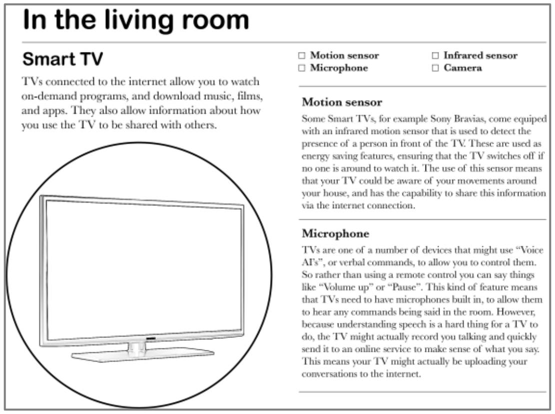
2.2 Awareness

Definitions of lying [17] presuppose a second party - an observer of the falsehood, or an intended target of the deception. It's impossible, theoretically, to lie in isolation. To consider lying to an object first requires an acknowledgement of the object as a potential interlocutor - that it has the capacity to receive and attend to information. A primary aim of the Countermeasures project is to provoke this acknowledgement amongst users.

In the context of contemporary private and public space, regarding surrounding objects as perceptive to information is both plausible and constructive. The combination of physical sensors and wireless connectivity in smart devices and 'internet of things' products [4] means that environments are increasingly likely to contain objects that are active observers of human behaviour. Sensors transduce physical actions into digital information, and connectivity allows this information to be perceived and considered by a broader range of remote systems. Together, the physical sensors and networked analysis form an extended digital sensorium attuned to human behaviour. While the inferences of the algorithmic parts of this sensorium are noted for their inscrutability, the practical sensing apparatus are also difficult to comprehend, despite their physical presence.

Acknowledging the intermediary role of sensor-enhanced objects encourages us to understand them in a different context. Such objects are not passive, but are active agents of observation for systems reliant on an incoming flow of information. The inclusion of sensors turns televisions into observing, rather than merely observed objects [22], central heating thermostats observe domestic behaviours on behalf of global technology firms [15], and sensor enhanced cars act as vigilant representatives of insurance companies [5]. Whether we are aware of it or not, sensor-enhanced objects of this sort receive information from us, and in doing so have the capacity to be lied to.

Beyond the fundamental awareness that objects could be the target of a lie, successful lying also requires some awareness of the nature of the recipient of the false information. To convince someone that something false is true requires a certain level of understanding of their nature [23]. How much do they already know? What are their motivations? What are they likely to believe or disbelieve? These are also pertinent questions to ask about sensor-enhanced objects. The hidden nature of sensors - often taking the form of miniature integrated circuits buried within the exterior housing of devices - means that users do not necessarily know much about their presence or capabilities. Without access to live data generated by these sensors it's difficult to understand what behaviours they are sensitive to, and the extent or limitations of their perceptive abilities.



In the living room

Smart TV

TVs connected to the internet allow you to watch on-demand programs, and download music, films, and apps. They also allow information about how you use the TV to be shared with others.

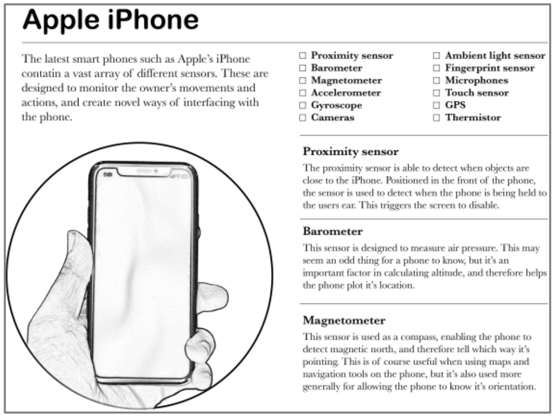
□ Motion sensor
□ Microphone
□ Infrared sensor
□ Camera

Motion sensor

Some Smart TVs, for example Sony Bravias, come equiped with an infrared motion sensor that is used to detect the presence of a person in front of the TV. These are used as energy saving features, ensuring that the TV switches off if no one is around to watch it. The use of this sensor means that your TV could be aware of your movements around your house, and has the capability to share this information via the internet connection.

Microphone

TVs are one of a number of devices that might use "Voice AI's", or verbal commands, to allow you to control them. So rather than using a remote control you can say things like "Volume up" or "Pause". This kind of feature means that TVs need to have microphones built in, to allow them to hear any commands being said in the room. However, because understanding speech is a hard thing for a TV to do, the TV might actually record you talking and quickly send it to an online service to make sense of what you say. This means your TV might actually be uploading your conversations to the internet.



Apple iPhone

The latest smart phones such as Apple's iPhone contatin a vast array of different sensors. These are designed to monitor the owner's movements and actions, and create novel ways of interfacing with the phone.

□ Proximity sensor
□ Barometer
□ Magnetometer
□ Accelerometer
□ Gyroscope
□ Cameras
□ Ambient light sensor
□ Fingerprint sensor
□ Microphones
□ Touch sensor
□ GPS
□ Thermistor

Proximity sensor

The proximity sensor is able to detect when objects are close to the iPhone. Positioned in the front of the phone, the sensor is used to detect when the phone is being held to the users ear. This triggers the screen to disable.

Barometer

This sensor is designed to measure air pressure. This may seem an odd thing for a phone to know, but it's an important factor in calculating altitude, and therefore helps the phone plot it's location.

Magnetometer

This sensor is used as a compass, enabling the phone to detect magnetic north, and therefore tell which way it's pointing. This is of course useful when using maps and navigation tools on the phone, but it's also used more generally for allowing the phone to know it's orientation.

Figure 2 and 3: Sample pages from the *I Spy Sensors* book. These pages give a description of sensors found in specific objects and guide to their functionality.
© Angus Main

The visible functionality of the object itself may only provide incomplete information about the nature of the sensing. For example, while a user may understand from using the interface that a smartphone contains a sensor that knows when it is being shaken back and forth, they are unlikely to know that the same sensor is so sensitive to vibration that it can act as a serviceable microphone [21]. Educating users to the presence and capabilities of these sensors is another core aim of this project.

The final area of awareness that the project seeks to encourage relates to the nature of the information itself. A conscious lie is the deliberate statement of false information. Logically, knowing what is false requires a liar to have an understanding of what represents a true statement. What is the 'true' information we currently already share with the sensor-enhanced objects that surround us? What data do we already allow to be generated about us, and how accurately does this reflect our behaviours? How might the existing information created by our actions be altered or subverted?

2.3 Agency

The use of hidden sensors in objects creates a power imbalance between the user and the manufacturer or service provider. It is a clear, contemporary example of the panopticon effect described by Bentham and Foucault [9]. As Foucault says of the hypothetical inmate of an architectural panopticon, "he is seen, but he does not see; he is the object of information, never a subject in communication" [9]. Similarly, the user of sensor-enhanced objects is engaged in constant communication, but without complete control over the nature of their contribution.

In the type of unilateral 'visibility trap' described by Foucault, the ability to lie represents a crucial degree of agency. It implies control over the flow of information from transmitter to receiver, and elevates the observed to an active subject in the communication.

Of the myriad different forms of lying and deception defined in law and linguistics, this project identifies three different categories which are applicable to lying to objects: falsification, omission, and obfuscation. Between them these three types of lie encompass the whole gamut of dishonesty, each undermining a separate tenet of society's model of truth - the oath of sworn testimony "to tell the truth, the whole truth, and nothing but the truth".

2.4 Omission - Telling the truth, but not the whole truth

Starting with the simplest to implement in the context of smart objects, to lie by omission is the selective exclusion of information to create a deceptive impression of events. Controlling the flow of information to include favourable data and omit unfavourable data is often achievable by simply blocking or obscuring the sensors on objects. For example, putting tape over a camera, motion sensor or microphone, or leaving the object in a different room, cupboard or refrigerator [7]. This is a blunt approach, but one that is already commonly used to manually disable webcams for privacy reasons [19] [6] [16].

There are several benefits to this approach. It's simple to achieve with minimal resources. It potentially reduces the information shared through a particular sensor to zero, making any kind of analysis or inference difficult. The manual nature of the intervention also provides the user with reassuringly physical evidence of the ongoing deception – i.e. 'if I can't see the camera lens through the tape, it can't see me'.

Deception by simple omission also has clear drawbacks. The 'believability' of the lie is limited as the deception is easily detectable. Sustained loss or reduction of signal within a system can be recognised and programmed for. Furthermore, as information is only being selectively withheld rather than actively fabricated, the user has only limited agency over information they are communicating with objects. Finally, as a method of deception this approach is only really viable for objects where a sensor is visible and accessible on the surface, such as a camera or microphone. It is less useful for sensors which operate obscured within an object, for example gyroscopes, accelerometers or barometers. For these types of sensors obfuscation may be a more successful form of lying.

2.5 Obfuscation - Telling the truth, and everything but the truth

Sworn testimony seeks 'nothing but the truth' as clarity is an imperative to truth. Conversely confusion is a useful vehicle for deception. True information can be lost, and deceptions created, if the truth is accompanied by a barrage of falsity. In informational terms adding random or unnecessary data to the communication increases entropy and makes it harder to determine signal from noise. Obfuscation is an approach already used in programming to prevent code from being read and understood by third parties by disrupting the flow of computation and artificially extending the content of the code [3] [18]. A similar approach can be taken to the disorientation of sensor-enhanced objects by deliberately targeting the sensors with excessive stimulus in order to obscure true readings in a stream of meaningless ones. For example, an accelerometer subjected to focused, persistent vibration from something like a haptic motor, is less likely to be able to detect any nuanced, natural movements of the object.

While this form of deception offers an opportunity to target embedded or less accessible sensors, and is potentially less detectable, it does require a more technical understanding of the sensors used in an object and the conditions required to activate them. Also, although it allows for more controlled deception than methods of omission, it still doesn't allow the user full control over the information they are communicating. For that the falsification approach is required.

2.6 Falsification - Telling your version of the truth

While omission and obfuscation allow for some information agency though deception, to achieve further control users would need the ability to manipulate sensors to generate specific information of their choosing. This would allow not just general deception, but outright lies - fabrications of specific untruths. Falsifying the information perceived by a sensor-enhanced object can be achieved in a number of ways, dependent on the nature of the sensor. A simple example would be using a strong magnet to affect a magnetometer and simulate a specific compass heading. More sophisticated sensors require more complex methods of falsification, for example spoofing a particular geolocation by falsifying a GPS signal [14]. This level of deception is more complex in terms of its application, requiring specific hardware and technical knowledge, but also more complex in terms of its impact. For example, successful falsification such as GPS spoofing can be undetectable by the object itself, and could have significant and undesirable consequences [14].

2.7 Moral Considerations

This project advocates lying and deception within the context of sensor-enhanced objects, and it would therefore be incomplete without consideration of the moral implications of these actions. The inherent immorality of lying can be taken for granted in many different contexts. However, the specific provocation for the deceptions described here is the inequity of power that sensors create by perceiving without being perceived. A usual requirement of lying in verbal or written forms is that a person makes a statement or declaration. In the normal use of a sensor enhanced object, no distinct 'statement' exists. Without the ability to directly control the sensors, all observable actions are potentially statements of information. This intrusive level of attention can be seen as a contravention of the normal expectations of communication, to which the deceptions described here are a countermeasure. The question to ask is whether these objects have 'a right to truth' [17], or whether this is negated by their nature.

Whilst users remain unaware of the full perceptive activities of the objects that surround them, then the process of deception is arguably started by the object itself. This is even before we consider sensor-enhanced objects which are specifically designed to lie to people, as demonstrated with the VW emissions scandal [12].

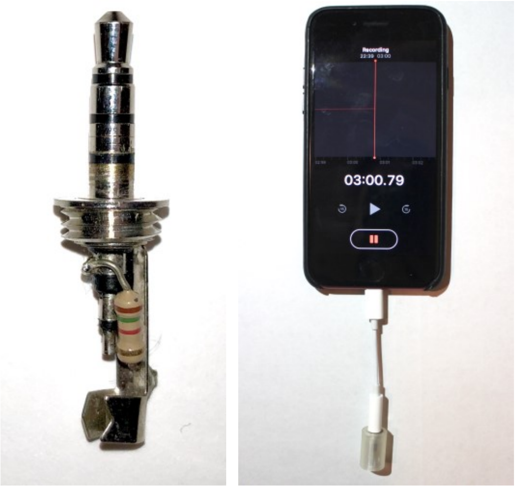


Figure 4 and 5: A microphone disabler. The left image shows the headphone jack without its case and the 1.5K Ohm resistor visible. The right image shows the device with 3D printed case attached, plugged into an iPhone 8 using the native lightning connector adapter.

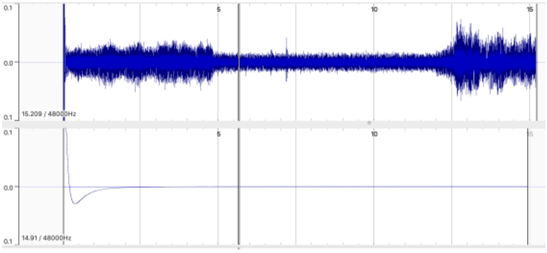


Figure 6: The waveform of two 15 second sound recording. The top waveform is a recording of ambient sound using an iPhone 8. The bottom waveform is a recording of the same sound on the same phone, but with the microphone disabler attached.

3 OUTCOME

To facilitate both awareness of and agency over sensor-enhanced objects, this project presents a range of design outcomes which aim to educate the users of these objects, and provide them with the means to create object-based deceptions. Awareness will be promoted through a custom designed guidebook to sensors, and agency through a toolkit of deception mechanisms.

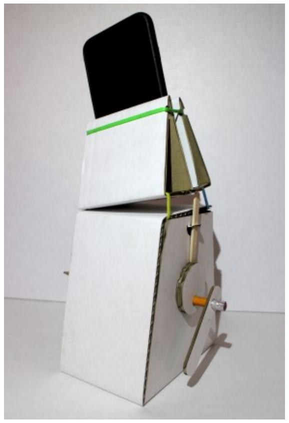
The project deliberately focuses on physical means of deception rather than software-based solutions. The intention of this is to demonstrably place control back in the hands of the user by keeping the tools in their realm of experience, rather than in the domain of the digital object. As Snowden and Huang note in the description of their physical counter-surveillance tool for phones [25], digital devices are open to hidden compromises and yet there are “no tools available through which one can determine what is happening beneath the glass and icons, preventing the development of a natural understanding of dangerous device states”. By using analogue tools there is the possibility that the physical affordances of the objects can reinforce awareness and agency, such as with the tape over a camera.

3.1 The Guidebook

Taking inspiration from children’s travel books and spotting guides such as Michelin’s I-Spy series of car journey activity books [13], the guidebook will present readers with a simple guide to recognising the presence of sensors in everyday situations and understanding more about their capabilities (fig. 1). In simulating the tone of familiar children’s books the aim is to present the information about complex technology in a non-technical, nostalgic, and accessible manner.

Following the format of such guides, the book presents images of the sensor-enhanced objects as they appear in the environment, and then further information about their capabilities, and how they could be deceived (fig. 2 and 3).

The guide book is intended as a form of critical design, inviting the reader to consider and question the proliferation of sensors in everyday objects, as well as offering a means of intervention. It covers a range of domestic and public spaces such as the kitchen, the living room, and the high street, as well as specific devices such as smart phones. Although the information contained in the guidebook could also be disseminated in a number of other forms, such as website or app, a print book has been chosen in order to aid distribution to non-technical audiences and underscore the projects emphasis on the physical.



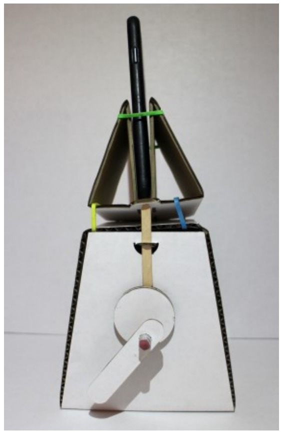


Figure 7 and 8: Two images of the Phone Jig. The laser cut cardboard device is easily assembled and allows the user to create repetitive physical actions to simulate behaviours like walking.

3.2 The liars tool bag

The tool bag consists of range of low-cost tools and materials to assist the deception of sensor-enhanced objects. The format and design of the tools is open source and could be replicated by individuals or organisation wishing to create their own versions. The inventory of included tools can be customised to suit particular contexts, but primarily includes tools for deceiving the sensors on smartphones. This is because smartphones represent the most common and most abundant source of sensors in daily life, and are therefore useful test beds for deception. The tools that can be included in the tool bag are:

Magnets, for falsifying magnetometer or compass data. This has been tested on iPhones using small Neodymium N42 magnets rated at a 2.7kg pull. A magnet in a stable position close to the phone causes the software compass to lock to a constant incorrect position (falsification). Moving the magnet around effectively disorientates the compass and prompts the software to request the user recalibrates (obfuscation).

Paper templates, for identifying the position of sensors within common smartphones. These are cut out paper sheets which can be placed directly on the back of the phone and indicate the location of specific sensors. Used in combination with the guide book and some of the other tools in the tool bag, this allows users to deceive particular sensors on their phone. Information is compiled from “teardown” analysis of devices. [27] [28].

Stickers, for covering cameras, infrared motions sensors, and microphones. These are simple, removable stickers which can be used in conjunction with the guide book.

Microphone disablers, a headphone jack with a 1.5k Ohm resistor attached to mimic the impedance of an external microphone, and cause the operating system to disable the internal microphones on digital devices (fig. 4 and 5). As the jack and resistor have no ability to sense sound, this effectively leaves the device listening to nothing. These disabling devices are low-cost and effective (fig. 6). However, they do rely on the devices software, and are therefore not a purely physical method of deception.

Phone jig, a cardboard actuator for a smartphone which physically moves the device in order to activate the accelerometer (fig. 7 and 8)). The principle of this is similar to existing critical design projects such as Studio NAND [26] and Unfit-bits [20], but in this case designed to produce specific deceptions using simple materials - corrugated cardboard, rubber bands, wooden sticks and a pencil. The jig comes with various sized cams which can be configured to move the articulated phone holder in various different ways. Users can create their own cams to simulate particular movements.

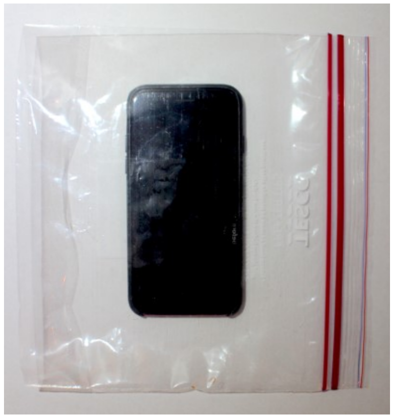


Figure 9: An iPhone inside a sealable plastic bag. This allows the user to control the air pressure around the phone.

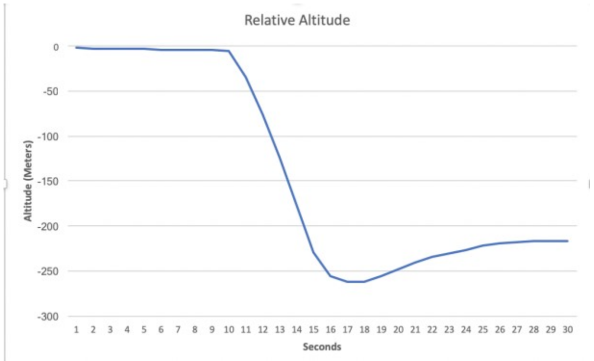


Figure 10: A graph showing the relative altitude readings from an iPhone 8's barometer sensor over a 30 second period. The phone had been sealed in a plastic bag with an air pocket inside. After 10 seconds, gentle pressure is applied to the sealed bag, resulting in dramatic change in altitude readings.

Sealable plastic bags, for controlling the air pressure in a smartphone and manipulating the barometric sensor. The plastic bag is a standard freezer bag, large enough to contain a phone (fig. 9). Sealing the phone inside allows the user to control the air pressure, which in turn is used to help calculate altitude. Sealing the phone in the bag with a large pocket of air, and then pressing gently on the bag causes the pressure to rise artificially. (fig. 10). The bag also provides a convenient container for the tools.

3.3 Conclusion

The guidebook and tool bag provide a starting point for creating awareness and agency over sensor-enhanced objects. They demonstrate that it's possible to counteract sensor components using simple physical tools.

The outcomes are not intended as conclusive solution, but a provocation, and a foundation for further activities. As sensor technology advances and becomes more pervasive, further countermeasures will be required. By disseminating these tools and concepts amongst the HCI community and broader user groups, the intention is that the project may gain further contributors and partners. It's important to acknowledge the limitations of such approaches – not all device users will be able to afford to use tools for deception and subversion, no matter the financial cost of the materials. However, it is hoped that the dialogue they provoke may extend further than just the physical outcomes, and that by framing these activities as lying, an implicit ethical question is raised which could prompt new approaches to our interactions with smart objects.

REFERENCES

[1] AdBlock. "AdBlock." *Surf the Web without Annoying Pop Ups and Ads!*, getadblock.com/.

[2] Altra. "TORIN IQ | Shop At Altra." *Altra Core 3 – Altra Running*, www.altrarunning.com/shop/men/torin-iq-alm1837q#hero=0.

[3] Balakrishnan, Arini, and Chloe Schulze. "Code Obfuscation Literature Survey." 19 Dec. 2005.

[4] Bastos, D., et al. "Internet of Things: A Survey of Technologies and Security Risks in Smart Home and City Environments." *Living in the Internet of Things: Cybersecurity of the IoT - 2018*, 2018, doi:10.1049/cp.2018.0030.

[5] "Black Boxes: Can You Trust Them to Lower Your Car Insurance?" *BBC*, BBC, 9 Nov. 2016, www.bbc.co.uk/news/uk-england-37910773.

[6] Boult, Adam. "Put Tape over Your Webcam, FBI Director Warns." *The Telegraph*, 15 Sept. 2016, www.telegraph.co.uk/technology/2016/09/15/put-tape-over-your-webcam-fbi-director-warns/.

[7] Bradsher, Keith. "Hasty Exit Started With Pizza Inside a Hong Kong Hideout." *The New York Times*, 24 June 2013, www.nytimes.com/2013/06/25/world/asia/snowden-departure-from-hong-kong.html.

[8] Cadwalladr, Carole, and Emma Graham-Harrison. " Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach."

[9] Foucault, Michel. *Discipline and Punish: the Birth of the Prison*. Vintage Books, 1995.

[10] Google. "Browse in Private - Computer." *Google Chrome Help*, Google, support.google.com/chrome/answer/95464?co=GENIE.Platform=Desktop&hl=en.

[11] Griffin Technology. “Griffin Technology Unveils Griffin Home, a Collection of Smart, AppPowered Appliances That Simplify and Enhance Everyday Routines at CES 2017 | Griffin Press.” *Griffin Technology Unveils Griffin Home, a Collection of Smart, AppPowered Appliances That Simplify and Enhance Everyday Routines at CES 2017 |Griffin*, press.griffintechnology.com/release/griffin-technology-unveils-griffin-home-a-collection-of-smart-apppowered-appliances-that-simplify-and-enhance-everyday-routines-at-ces-2017/.

[12] Hotten, Russell. “Volkswagen: The Scandal Explained.” *BBC*, BBC, 10 Dec. 2015, www.bbc.co.uk/news/business-34324772.

[13] “I-Spy (Michelin).” *Wikipedia*, Wikimedia Foundation, 3 Oct. 2018, en.wikipedia.org/wiki/I-Spy_(Michelin).

[14] Jafarnia-Jahromi, Ali, et al. “GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques.” *International Journal of Navigation and Observation*, vol. 2012, 2012, pp. 1–16., doi:10.1155/2012/127072.

[15] Kelion, Leo. “Google-Nest Merger Raises Privacy Issues.” *BBC*, BBC, 8 Feb. 2018, www.bbc.co.uk/news/technology-42989073.

[16] “Laptop Camera Cover Set.” *Electronic Frontier Foundation*, supporters.eff.org/shop/laptop-camera-cover-set.

[17] Mahon, James Edwin. “The Definition of Lying and Deception.” *Stanford Encyclopedia of Philosophy*, Stanford University, 21 Feb. 2008, plato.stanford.edu/entries/lying-definition/.

[18] Majumdar, Anirban, et al. “A Survey of Control-Flow Obfuscations.” *Information Systems Security Lecture Notes in Computer Science*, 2006, pp. 353–356., doi:10.1007/11961635_26.

[19] “Mark Zuckerberg Masks Mac Webcam and Microphone.” *BBC*, BBC, 22 June 2016, www.bbc.co.uk/news/technology-36596070.

[20] Mattu, Surya. “Unfit Bits.” *Unfit-Bits*, 2015, www.unfitbits.com/.

[21] Michalevsky, Yan, et al. “Gyrophone: Recognizing Speech from Gyroscope Signals.” *USENIX Security Symposium*, Aug. 2014, pp. 1053–1063.

[22] “Not in Front of the Telly: Warning over 'Listening' TV.” *BBC*, BBC, 9 Feb. 2015, www.bbc.co.uk/news/technology-31296188.

[23] Pruss, Alexander R. “Lying and Speaking Your Interlocutor’s Language.” *The Thomist: A Speculative Quarterly Review*, vol. 63, no. 3, 1999, pp. 439–453., doi:10.1353/tho.1999.0016.

[24] Sannon, Shruti, et al. “Privacy Lies: Understanding How, When, and Why People Lie to Protect Their Privacy in Multiple Online Contexts” *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI 18*, 2018, doi:10.1145/3173574.3173626.

[25] Snowden, Edward, and Bunnie Huang. “Against the Law: Countering Lawful Abuses of Digital Surveillance.” *PubPub*, 2016, doi:10.21428/12268.

[26] Studio NAND. “Unreliable Machinery for Design Fiction.” *Studio NAND*, nand.io/projects/unreliable-machinery.

[27] “Teardowns.” *IFixit*, www.ifixit.com/Teardown/.

[28] techinsights.com. “Apple IPhone Xs Max Teardown.” *TechInsights*, www.techinsights.com/about-techinsights/overview/blog/apple-iphone-xs-teardown/.

[29] Yale. “Conexis L1 Smart Door Lock.” *Yale.co.uk*, ASSA ABLOY, www.yale.co.uk/en/yale/couk/products/smart-living/smart-door-locks/conexis-l1-smart-door-lock/.