Internet Society Policy Brief:
IoT Privacy for Policymakers

September 2019

Introduction

The Internet of Things, or IoT, is the latest wave of integration of technology into our lives and surroundings. This rapidly-spreading new generation of devices brings cameras, microphones, sensors, computing, and network access into non-computer products. It extends into the home, retail and public spaces, enabling new forms of interaction, entertainment, commerce, and communication.

Connected devices undermine a fundamental principle of privacy: the ability to keep contexts separate from one another as we choose. This is especially significant in the case of home and wearable IoT devices, because of the strong presumptions of privacy we associate with the contexts of home and body.

There are many estimates as to the value and size of the IoT market,[1] but it is enough to say that their social and economic impact will be significant, and the spaces we inhabit are becoming more populated with 'connected' devices.

While consumer IoT devices will undoubtedly be fun and may enhance our daily lives, they will also introduce a host of new privacy issues, and amplify existing ones. IoT devices will encroach upon traditionally private spaces such as the home, and extend the data collection practices of the online world into the offline world. The number and nature of sensors being introduced will bring data collection ever closer to our bodies and intimate spaces. The intimacy and ubiquity of IoT will raise issues of control, consent and transparency, and increasingly erode the boundary between the private and the public spheres.

This policy brief identifies the key privacy challenges and risks arising from IoT devices in our homes, workplaces, public spaces, and on our person. We make recommendations for affirmative actions that policymakers, IoT service providers and other stakeholders can take to address these challenges. The primary scope is consumer IoT, though many of the key considerations and recommendations can be applied more broadly. This document also serves as a complement to the Internet Society's policy brief on IoT security.[2]

What is the Internet of Things (IoT)?[3]

While there is no single, agreed-upon definition, for the purposes of this paper the term "Internet of Things" refers to "scenarios where network connectivity and computing capability extends to objects, sensors and everyday items not normally considered computers, allowing these devices to generate, exchange and consume data with minimal human intervention."[4] IoT includes consumer products, durable goods, cars and trucks, industrial and utility components, sensors, and more. It presents a new way for users to interact with the network, using devices that are not limited to traditional computers, smartphones, and laptops.

1 IBM forecast one trillion connected devices by 2015: "Making Markets: Smarter Planet," IBM Investor Briefing, May 9, 2012, https://www.ibm.com/investor/events/investor0512.html; in 2011 Cisco anticipated 50 billion devices by 2020: "The Internet of Things: How the Next Evolution of the Internet Is Changing Everything," Cisco White Paper, https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf; Gartner Research claimed 8.4 billion devices in 2017 and expect 20 billion in 2020: "Gartner Says 8.4 Billion Connected 'Things' Will Be in Use in 2017, Up 31 Percent From 2016", https://www.gartner.com/newsroom/id/3598917

2 https://www.internetsociety.org/wp-content/uploads/2018/04/IoT-Security-for-Policymakers_20180419-EN.pdf

3 For more Internet Society resources, see our IoT page (https://www.internetsociety.org/iot/) and "The Internet of Things (IoT): An Overview" linked from that page.

4 https://www.internetsociety.org/doc/iot-overview

What is privacy, in the context of IoT?

Privacy is a key factor in trust relationships. When we disclose data to others, we are (implicitly or otherwise) trusting them not to use it in ways that conflict with our interests. As we will note in the following section, privacy is linked to the context in which we disclose data. In the context of IoT, privacy boils down to two things: either we trust third parties not to abuse the data generated by our use of connected objects, or we rely on the ability to control the collection and use of that data. In the IoT domain, privacy therefore carries strong implications of trust, transparency and control:

- The ability for individuals to control how the information collected by their IoT devices is shared, and determine who has access to the data from devices in your home, in your car, and on your person. This means easy ways to blind and mute devices, and to have a say in how IoT data is analyzed or shared with third parties.

- Clarity about how information about people is collected, used, and shared with others. IoT devices and their applications should enable the user to find out what information is collected and shared, when and with whom.

- The ability to determine how identifiable one is when undertaking online or offline activities. IoT devices should have the option for pseudonymous or anonymous use.

- The ability to control one's digital footprint[5], especially from IoT devices in intimate settings. The user should understand where information about them has gone, and how long it is kept.

Privacy is a social value as well as an individualistic one: it supports and empowers people with the option to withdraw from the gaze of, and interactions with, others at will, and the right to respect for their personal space, to create solitude and reserve from others.[6] This right is reflected in both the Universal Declaration of Human Rights (UDHR, Article 12[7]) and the European Convention on Human Rights (ECHR, Article 8[8]).

In keeping with this right to privacy, individuals should be able to enjoy the benefits of consumer IoT either with as little privacy risk as possible, or having made a clear, informed judgement about risk and benefit. Consumer trust in IoT potentially affects consumer trust in general, and trust in the Internet in particular. Championing strong user control and meaningful choice, better notification methods, greater transparency, and fit-for-purpose governance instruments will help safeguard privacy and trust in the IoT.

5 Your digital footprint is the "trail" you leave behind as you use the Internet. Comments on social media, VOIP calls, app use and email records - it's part of your online history and can potentially be seen by other people, or tracked in a database. https://www.internetsociety.org/tutorials/your-digital-footprint-matters/

6 Law review article published in 1890 by Samuel Warren and (later US Supreme Court Justice) Louis Brandeis, as cited in Arizona Law Review article The Invention of the Right to Privacy http://law.scu.edu/wp-content/uploads/Privacy.pdf

7 " No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation." - UDHR, Art.12

8 "Everyone has the right to respect for his private and family life, his home and his correspondence." - ECHR, Art.8

Key Considerations

IoT is characterised by a number of factors:

- Scale (the sheer number of devices, objects, sensors and imbedded systems)
- Proximity (the intimacy of devices such as wearables and implants)
- Ubiquity (the mass deployment of IoT in public and private spaces)
- Connectedness (which is not the same as device intelligence!)

These factors have an impact on privacy. They make it easier for the individual to be:

- Identified
- Tracked
- Profiled
- Influenced

IoT amplifies existing privacy challenges and creates new ones.

IoT is typified by increased sensor scale and proximity. The decreasing cost - both of sensors and of the computational cost of collecting, analyzing, and sharing their data - is fueling a proliferation of cameras, microphones, infrared detectors, accelerometers and other sensor technologies. The scale and diversity of sensors entering the human environment is greater than we have ever known. Related to this is the proximity of these sensors to the human body, allowing close-up monitoring of people's faces, bodies and movement.

1. Increased sensor scale and proximity creates the potential for continuous monitoring of people's activities, behaviors, speech, health and emotions. While some IoT devices don't begin monitoring until a "wake word" is uttered (i.e. "voice-activated") or after being manually activated (i.e. "physical switch"), others will probably be "always-on", always sensing, watching, and listening without any user intervention[9]. Further, as people become more desensitized to these devices, they will become less aware of being monitored by them; the devices will fade into the background.

2. IoT will make people more identifiable in public and private spaces. One of the most ubiquitous IoT sensors is the camera. Tiny cameras can already see detail very clearly. Coupled with advances in facial recognition and other analytic-technology, IoT devices will allow people to be identified or singled out wherever these cameras are present. As a cloud service, facial recognition is likely to be cheaply available to many IoT manufacturers and service providers.

3. IoT devices are connected, but not necessarily "smart". Virtual assistants like Amazon's Alexa, smart TVs with cameras and microphones, Internet-connected toys, and in-home security devices allow IoT companies to penetrate the walls of the home, a traditionally private space. Because the devices are "dumb", the data they collect is often processed elsewhere: it leaves the supposedly private context of the home, and can be seen, mined and shared by third parties.

9 See Future of Privacy Forum work - https://fpf.org/wp-content/uploads/2016/04/FPF_Always_On_WP.pdf

4. This, in turn, tends to lead to “siloed”, proprietary IoT products and services:

    a. A connected heart monitor from one manufacturer might only talk to the server and/or diagnostic terminal of that manufacturer – not one of the patient’s choosing.

    b. Different connected devices in the same household might each insist on their own manufacturer’s device controller, rather than sharing a single controller of the consumer’s choosing.

5. Factors such as these reduce consumer choice, increase vendor lock-in, and can make monopolistic behaviour and/or market failure more likely.

6. IoT shrinks private spaces generally. The combination of the above trends – sensor scale and proximity, continuous monitoring, increased identifiability, and the breaching of the walls of the home – points to a potential decrease in people’s ability to find private places of reserve and solitude generally.

7. IoT will enable and normalize increased online behavior tracking in the offline world. Connected devices break down the boundary between the online world and spaces which people may still think of as offline and therefore private. When Helen Nissenbaum[10] referred to privacy as "contextual integrity", she was referring to the individual's ability to keep such boundaries in place when they choose to do so. Making human behavior in the offline world visible to commercial analysis could enhance manipulation of consumers, make people feel vulnerable, and create more valuable stores of personal data to share, sell, or be stolen.

8. Privacy protection is a key pillar supporting trust in IoT and our interactions with it. Trust in IoT’s key actors – service providers, infrastructure companies, retailers, governments, and manufacturers – is necessary to realize the benefits of the coming waves of connected devices. Privacy is a fundamental aspect of building that trust. IoT devices will collect a range of new personal data and behaviors – consumers must trust that the custodians of this data will treat it, and them, respectfully. In the absence of this trust, people won’t embrace IoT devices, fearful that their data will be insecure or shared inappropriately.

The Common Theme of Context

These examples illustrate the way in which ubiquitous, often inconspicuous devices represent a fundamental change in our concept of "context". Where the home used to be a private space, IoT now makes it accessible to third parties - even, sometimes, with no action on the part of the individual: if I visit a friend, how am I to know that his connected devices are capturing and processing our conversation? If I give my child a 'talking doll', am I in fact introducing a commercial third party into that child's bedroom?

Connected devices undermine a fundamental principle of privacy: the ability to keep contexts separate from one another as we choose. This is especially significant in the case of home and wearable IoT devices, because of the strong presumptions of privacy we associate with the contexts of home and body.

10 Privacy as Contextual Integrity - Helen Nissenbaum, Washington Law Review, 2004 https://crypto.stanford.edu/portia/papers/RevnissenbaumDTP31.pdf

Challenges

IoT crosses sectoral and jurisdictional regulatory boundaries.

In some countries, like the United States, privacy and data protection rules tend to be divided into silos: medical privacy, financial privacy, student privacy, and so on. IoT devices and services, however, do not fall neatly into regulatory categories.

For example, consumer wearable devices might generate health information, but not be covered by medical data laws. Cars are subject to many forms of regulation (safety, environmental, etc.), but none of those will necessarily cover the privacy aspects of connected vehicles and the data to which they give rise.

Similarly, some regions, countries, states, or cities may decide to regulate different privacy aspects of IoT devices and services, in ways that do not apply outside those areas.[11]

This challenge is greatly amplified by the distributed nature of the Internet. Collection, processing, interpretation and application of the resulting data could all take place in different jurisdictions, with different applicable rules and regulations.

IoT makes it harder to obtain informed consent.

Wherever IoT is deployed – in the home, in retail spaces, in public areas – people's faces, identities, and utterances can be collected. For everyone except the device owner, gaining informed consent to be recorded will be almost impossible. Even for the device owner, this is compounded by the fact that, for many IoT devices, the interface exposed to the user neither reveals, nor offers control over the data and functionality available to the service provider.

It's a challenge to make people aware of the presence of IoT devices, particularly when they are in spaces controlled by others, and especially hard to give people the ability to opt out of passive data collection.

IoT blurs the notion of private and public.

Wearable devices go with people from their home to their car to their place of work to where they socialize[12]. IoT devices in the home share data with third parties outside the home. People entering someone else's home (or other public or private space) may not be aware that their image, voice, or actions are being recorded and transmitted to third parties. Activities in the home will become datafied[13] and transmitted as soon as they are collected.

IoT devices are designed to be unobtrusive.

One of the key selling points of IoT devices is that they look like familiar things: watches, clock radios, speakers, televisions, bathroom scales, and so on. Cameras and microphones are often merely tiny black circles or holes in the device. As such, their monitoring and recording capabilities are often opaque and hidden. There may be little or no indication of when the device is recording, what is happening to the resulting information, where is it sent, who has access to it, how its use can be controlled, and whether it can be deleted.

---

11 A recent example in California (US) is their IoT privacy bill https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327

12 French intelligence staff geolocated by their fitness trackers: https://www.rtl.fr/actu/futur/des-agents-de-la-dgse-localises-jusqu-en-irak-a-cause-d-une-application-de-running-7792366670

13 Datafication refers to the transformation of attributes, activities and behaviors in the physical world into data that can be readily analyzed. See http://ide.mit.edu/news-blog/blog/datafication-business-and-society

IoT challenges the principle of transparency.

The principle of transparency[14] is embedded in most privacy and data protection frameworks - but some characteristics of IoT are at odds with this principle.

1. IoT devices present user notification and comprehension challenges.

   Since consumer IoT devices are often small and resemble the connectionless devices they replace, they often do not have much in the way of screens or other user interfaces, although some connect to apps on smartphones for this purpose. This causes several problems.

   First, unlike websites, many IoT devices have no practical way to display their privacy policies – at best these are included in their packaging, and at worst they are only accessible after opening and installing the device (with many smart TVs as a prominent example[15]) - or there may be a link to the manufacturer's website somewhere in the documentation.

   Second, IoT devices may not have good ways of notifying people that they are collecting data, or, as in the case of driving, may not be able to notify at certain times due to valid concerns about causing harm to users, such as by distracting drivers. To make matters worse, emerging research shows that some IoT service providers' privacy policy statements are hard to find, vague about device capabilities, and opaque about data collection.[16]

2. As more devices are introduced with IoT features, it will be harder for consumers to decline those features.

   As the cost, size, and complexity of including sensors and networking capabilities continues to fall and become normalized, certain products may simply no longer be available in 'dumb' versions. Consumers cannot "vote with their wallets" if there's no privacy-respecting alternative on the market.

3. IoT has an impact on children.

   Devices in the home and in public generally do not discriminate well between adults and children. An Amazon Echo picks up the voices of children as it does adults.[17] High profile news stories about connected toys reveal serious security vulnerabilities that could put children at risk.[18]

   As the human environment becomes more saturated with sensors and microphones, children's activities and data are at risk of indiscriminate collection and monitoring, by commercial third parties whose presence and role are not evident to the individual.

---

14 See, for example, Article 29 Working Party, "Guidelines on transparency under Regulation 2016/679" at http://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025

15 See Peppet, "Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security & Consent", pp. 131-132 at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2409074

16 See Rosner and Kenneally, "Clearly Opaque: Privacy Risks of the Internet of Things," pp. 56-59 at https://www.iotprivacyforum.org/clearlyopaque/

17 Amazon has released a child-specific version of the Echo called Echo Dot Kids Edition, prompting two members of the US Congress to ask Amazon about its privacy characteristics: https://www.markey.senate.gov/imo/media/doc/Amazon%20Echo%20Dot%20Kids%20Edition.pdf

18 See e.g., de Freytas-Tamura, "The Bright-Eyed Talking Doll That Just Might Be a Spy" at https://www.nytimes.com/2017/02/17/technology/cayla-talking-doll-hackers.html

Guiding Principles and Recommendations

The above-mentioned challenges require action by multiple stakeholders - sometimes collaboratively (such as on guidance, consent and market choice). Many privacy measures and risk mitigations, in particular, require collaborative action by multiple stakeholder groups.

Accordingly, in this section, we set out a number of principles and actions, which apply across the stakeholder groups. These include governments, service providers, data controllers and the supply chain of designers, manufacturers and implementers who bring IoT products and services to the consumer market. The recommendations apply to all those developing and implementing privacy policy for consumer IoT, whether through laws, industry self-regulation, corporate privacy policies, or privacy standards.

Where appropriate, we relate recommendations to the corresponding principle in the Internet Society/Online Trust Alliance IoT Trust Framework.

Because of the pervasive nature of IoT, governments have a role to play in ensuring that devices and services do not expose citizens to individual or collective risk, harm privacy, or exacerbate vulnerability or discrimination. That role may involve both direct intervention (through legislation and regulation), and indirect intervention - encouraging, motivating and empowering other key stakeholders to play their respective roles. For example, governments can facilitate consumer education, awareness-raising, and understanding of privacy risks and mitigations, even if the education itself is provided by other parties.

Governments can also promote self-regulation, as one approach towards ensuring that service providers respect consumers' interests and cultivate the trust needed for market acceptance.

In cases where market forces, on their own, fail to provide a compelling incentive for service providers and data controllers to improve best practice, government intervention may be appropriate to prevent or correct for market failure - for instance to ensure that bad actors are held accountable for poor data handling practices, or that consumer protection laws are effectively enforced. The role of market forces in IoT is examined in the Internet Society paper "Economics of Security of Consumer Grade IoT Products and Services".

Enhance User Control

Principle: Enhance Meaningful User Control of IoT Devices and Services, and the Management of the Data They Collect

- Ensure that regulations define clear and robust responsibilities for service providers.
    - Require companies to gain informed consent to collection of personal data before first use of a device – merely unwrapping a box should not imply consent.
    - Informed consent requires transparency - for instance, about data-sharing with third parties.
    - Third-parties should be held to the same privacy standards as the service provider itself, with the service provider ultimately responsible. Where a service provider shares or outsources data to another entity, that should not dilute the privacy obligations of either of them.[19] If an

19 Internet Society / Online Trust Alliance (OTA) IoT Trust Framework Principle #25 https://www.internetsociety.org/resources/doc/2018/iot-trust-framework-v2-5/

individual requests deletion of personal data, it is up to the service provider to ensure that the data concerned is deleted by third parties as well.

- Service providers should store data securely, limiting access only to those with a justifiable business need, and with a duty of notification in case of data loss or unauthorized access.

- Encourage open standards and interoperability in IoT products and services.
  - Promote open, interoperable specifications and architectures versus closed, proprietary ones.
  - IoT manufacturers should be encouraged to publish interfaces to their devices, controllers and servers, and increase the interoperability of data generated by their devices.
  - This will open up markets for value-added services, increase user choice, and improve the prospects of transparency and effective user control[20].

- Encourage or require data minimization.
  - Champion opted-out by default versus opted-in by default.
  - Data minimization is a key element of privacy by design. It is also in the interest of the data controller to minimize the regulatory and reputational risks that arise from holding personal data. IoT will generate massive amounts of data, tempting companies to collect and mine everything they can, even if that was not the consumer's expectation in buying the product.
  - Industry regulation, whether through legislation or industry codes of conduct, should reflect users interests by limiting collection, use and retention to the minimum necessary to deliver the service the user expects.
  - Selective sharing. In many cases, IoT data is meant to be selectively shared by a device's owner: with friends, with fitness coaches, with doctors, with family members. IoT device interactions and management consoles should be designed to make it easy for the user to understand and control the sharing, e.g. allowing the data to be shared with this person but not that person, and for a particular period of time.
  - Limits on data retention. Service providers should allow consumers to request deletion or anonymization of personal or sensitive data once it is no longer needed for use of the product or service.
  - The consumer should also be able to delete data on the device itself upon discontinuing use, loss, or sale of a device.[21] Service providers should offer the ability to reset a device and accompanying applications to factory settings, including the ability to erase user data, so that devices can be safely decommissioned at their end of life.[22]

20 https://open-stand.org/open-standards-vs-proprietary-are-open-standards-really-the-wave-of-the-future-for-iot/

21 Internet Society / OTA IoT Trust Framework Principle #32

22 Internet Society / OTA IoT Trust Framework Principle #33

- Take care that children and other vulnerable consumers are not put at risk.
    - Networked toys, virtual in-home assistants, and smart televisions will all collect children's personal data. Parents have always had the burden of managing their children's privacy – IoT will increase that burden. Require improved notification (see "Transparency and Notification" below) of what children's data is collected and how it's used, to make it easier for parents to delete data from devices and services. Ensure tighter regulatory scrutiny of child-specific products (like toys and baby monitors).
    - Other vulnerable consumers, like children, may make it necessary for a guardian or other responsible adult to be able to act as a proxy.

Designing better privacy interfaces for constrained devices

Privacy by design (PbD) empowers users by giving them 'agency': the ability to shape their informational lives, the flow of their personal data and the data collection environment they inhabit.

IoT devices can and should do more to help users see and control the data their devices generate - but this takes careful design. Controls that are too detailed may offer great protection, but if they reduce convenience and are hard to use, users are likely to ignore them.

Designers devote great ingenuity to making IoT devices useful and convenient: they should apply the same creativity to the design of privacy controls.

Improve Transparency and Notification

Principle: Information to users should enhance transparency and control by being clear, accurate, relevant, and appropriately detailed.

- Improve the way users are notified about IoT devices' capabilities and data gathering.
    - Stimulate research into best-of-breed IoT notification practices, and encourage privacy regulators to publish guidance on how companies can experiment with different forms of notification while still complying with regulations. Without such guidance, companies may be reluctant to alter their existing notification practices, or amend their privacy policy statements in ways that make them easier to understand.[23] (Corresponding requirements for service providers are described below).

23 See US Federal Trade Commission (FTC) Workshop, "Putting Disclosures to the Test," at https://www.ftc.gov/news-events/events-calendar/2016/09/putting-disclosures-test ; and Schaub, et al., "A Design Space for Effective Privacy Notices," at https://www.usenix.org/system/files/conference/soups2015/soups15-paper-schaub.pdf

- Meaningful consent and opt-out
    - Review consumer protection measures to ensure they address IoT-related issues. For example, users should have effective recourse if privacy terms are not conspicuously disclosed prior to purchase.[24]
    - Ideally, connected products should still be usable even if the consumer opts out of data collection/sharing. If opting out significantly reduces the function or usefulness of the product, this should be clear to the user before purchase (if "fitness for purpose" rights are already in place, these may be applicable here).[25]
    - Where consent for data collection is a condition of being able to use the product, that consent should not be considered to have been freely given.
- Clarity of privacy policies
    - The privacy policies which apply to IoT products must be publicly available, and easy to find and understand. They should include details of personal data retention policies and periods.[26]
    - Changes to privacy policies should be clearly posted – best practices include date stamping, redlines, and summary of the impacts of the changes.[27] [28]
- Clarity for the consumer at the point of choice
    - It should be clear to the consumer, at the point of choice, what sensors a device has, what control the consumer has over their activation, and where the device stores the data it uses/generates (i.e. does it leave the device?). This is analogous to the "subscription required" caveat for digital content delivery.
    - Retailers should encourage manufacturers to view enhanced privacy as a product differentiator.
- Transparency throughout the data lifecycle
    - The consumer must have convenient means to discover what data the device produces/discloses, how it is used, for how long, and what inferences are drawn from it.
    - As mentioned above, the service provider's responsibilities should persist when personal data is shared with third parties, and third parties should "inherit" the same responsibilities.

24 Internet Society / OTA IoT Trust Framework Principle #28
25 Internet Society / OTA IoT Trust Framework Principle #29
26 Internet Society / OTA IoT Trust Framework Principle #22
27 Internet Society / OTA IoT Trust Framework Principle #31
28 See for example The Usable Privacy Policy Project: https://www.usableprivacy.org/, https://explore.usableprivacy.org/?view=machine

- Privacy and security throughout the product lifecycle.
    - The consumer should be given clear information concerning the duration of security and patch support (beyond product warranty).[29] This should include what happens when the device no longer receives security updates or if the user fails to update the device.[30]

Keep Pace with Technology

Principle: Update privacy laws and policies to reflect the new world of pervasive sensors and continuous monitoring.

- Review existing privacy, data protection and consumer protection laws and policies for fitness.
    - Current laws may not always consider sensor data as needing privacy protection, even though such data can often be made identifiable with little effort.[31] Privacy and data protection laws need to take into account the potentially revealing nature of sensor data and ensure that strong privacy protections apply.
- Improve the longevity and scope of privacy/data protection laws and policies
    - Where a single, overarching privacy/data protection law is not in place, consider passing one that covers collection and use of personal data from a technology-neutral perspective. Even where over-arching and/or sectoral laws are already in place, additional sectoral privacy laws for specific industries may be needed for greater legal certainty, or to address new risks specific to the emerging IoT market (e.g. connected devices with a high degree of autonomy, such as driverless vehicles; or pervasive sensors in public spaces).
- Strengthen legal protections for privacy researchers.
    - Ensure that privacy researchers are not put at legal risk for investigating privacy vulnerabilities. As with security researchers, privacy researchers must feel safe that they will not be in any legal jeopardy from seeking out and publishing information about privacy flaws in IoT devices[32]. If researchers are reluctant to investigate, many IoT privacy problems could persist unnecessarily.
- Ensure that discrimination and unfair practices are not boosted by the advent of IoT.
    - Explore legislative and regulatory methods to restrict certain kinds of IoT data from being seen or used by specific parties. For example, to prevent insurance companies from using IoT-derived data as a factor in insurance rates, unless explicit, informed consent has been freely given.

29 Internet Society / OTA IoT Trust Framework Principle #19

30 Internet Society / OTA IoT Trust Framework Principle #21

31 See Peppet, "Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security & Consent", pp. 131-132 at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2409074

32 For instance, researchers might reverse engineer a proprietary IoT system in order to be able to monitor the behavior, communications patterns and data disclosures of a device.

- Use government procurement practices and market strength to lead by example.
    - Build strong privacy requirements and privacy impact assessments into government IoT device and service contracts, to shape industry norms and encourage good practice.
- Privacy Impact Assessments in the IoT Development Process.
    - Following principles of value-based design, IoT product/service development should incorporate privacy impact assessments, to assess and mitigate the privacy risk to consumers as part of the design.

Strengthen the Multi-stakeholder Approach to IoT Privacy

Principle: Address the diversity of IoT risks and benefits, by broadening the range of participants in the IoT governance debate.

- Cultivate a broad range of dialogue.
    - Civil society groups, the public, government, advocates, commercial industry, academics, and technologists should convene to acknowledge differing stakeholder perspectives and priorities, and to identify IoT privacy issues and possible mitigations.
- Strengthen the voice of the consumer.
    - Consumers are likely to need some help in being heard at equal volume to an increasingly pervasive and economically powerful industry, whether directly or through their advocacy proxies in civil society and consumer protection.
    - The discourse of IoT is typified by descriptions of how much economic and social benefit it will yield. However, since IoT also introduces risk - sometimes at massive scale, the precautionary principle should also apply: the "sales pitches" should be balanced with the voices of those who hold wary and contrary views, and those who are focused on ensuring respectful and fair treatment of consumers, people of low socioeconomic status, and marginal communities.
    - IoT innovation may not be beneficial to all consumers, so there must be active inclusion of groups who will point out particularly vulnerable stakeholders, or practices that could harm individuals' privacy and society.

IoT is poised to transform economies and societies worldwide. The technology brings enormous opportunities but also significant risks. We are at a critical moment when we need to take steps to ensure that the benefits of IoT outweigh the privacy risks, but that will require collaborative effort from all stakeholders, including policymakers, manufacturers, and consumers, so that the opportunities represented by IoT are sustainably and responsibly developed.

Appendix: Further Reading

Internet Society, IoT Security for Policymakers (2018), https://www.internetsociety.org/wp-content/uploads/2018/04/IoT-Security-for-Policymakers_20180419-EN.pdf

Internet Society, OTA IoT Trust Framework (2018), https://www.internetsociety.org/iot/trust-framework/

Gilad Rosner and Erin Kenneally, Privacy and the Internet of Things: Emerging Frameworks for Policy and Design (2018), https://cltc.berkeley.edu/wp-content/uploads/2018/06/CLTC_Privacy_of_the_IoT-1.pdf

Scott Peppet, Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security & Consent (2014), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2409074

Broadband Internet Technical Advisory Group (BITAG), Internet of Things Security and Privacy Recommendations (2016), http://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf

Office of the Privacy Commissioner of Canada, The Internet of Things: An introduction to privacy issues with a focus on the retail and home environments (2016), https://www.priv.gc.ca/media/1808/iot_201602_e.pdf

US Federal Trade Commission, Internet of Things: Privacy & Security in a Connected World (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

US National Telecommunications and Information Administration, Fostering the Advancement of the Internet of Things (2017),