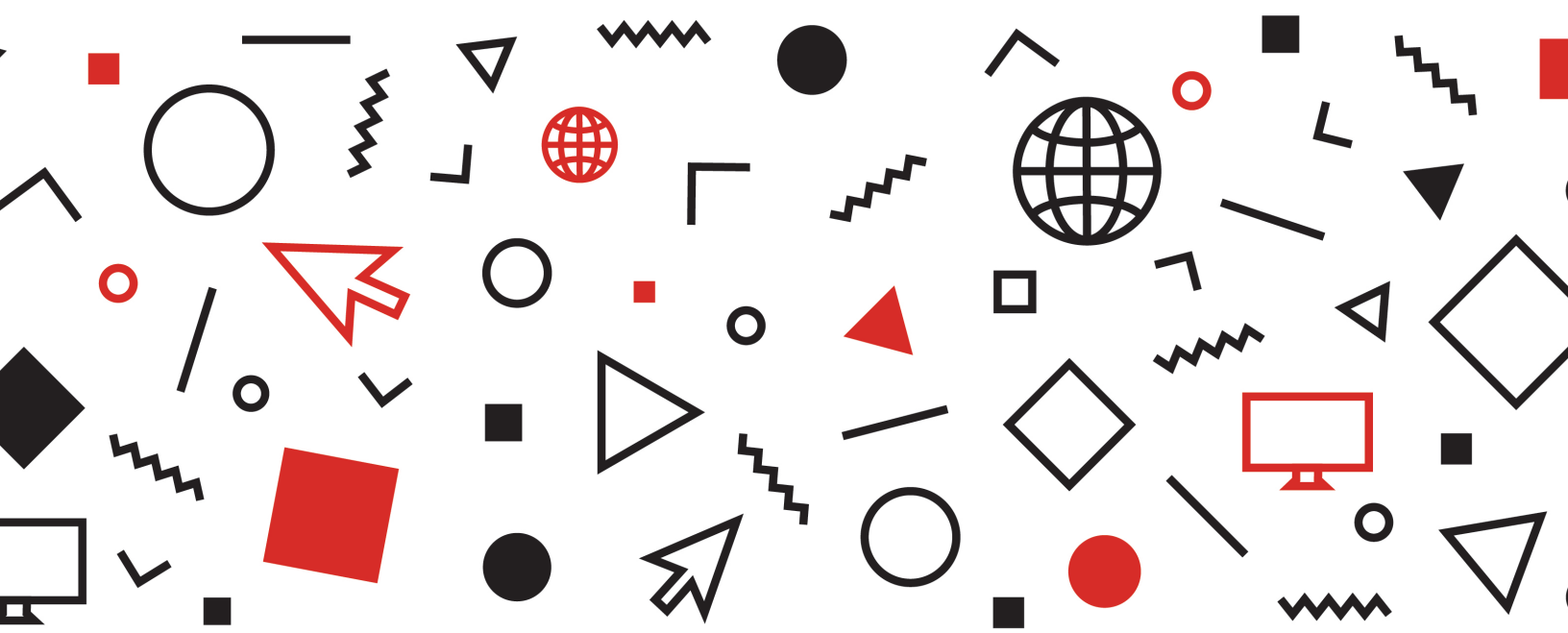

YOUTH AND THE INTERNET OF THINGS IN CANADA

PERSPECTIVES ON PRIVACY, SECURITY, AND ENGAGEMENT IN THE DIGITAL AGE

PREPARED BY THE YOUTH INTERNET GOVERNANCE FORUM FOR THE CANADIAN MULTISTAKEHOLDER PROCESS ON ENHANCING IOT SECURITY

YOUTH IGF CANADA

Youth IGF in Canada

Youth IGF Canada aims to increase awareness of internet governance issues and facilitate youth participation in global policy-making at the IGF and beyond.

Internet Society

The Internet Society is a global cause-driven organization governed by a diverse Board of Trustees that is dedicated to ensuring that the Internet stays open, transparent and defined by you.

Canadian Multistakeholder Process on Enhancing IoT Security

The Internet Society has partnered with Innovation, Science and Economic Development, the Canadian Internet Registration Authority, CANARIE, and CIPPIC to convene stakeholders in order to develop recommendations for a set of norms/policy to secure the Internet of Things in Canada.

This report was made possible through funding by a Youth Engagement Grant from the Internet Society as a part of the Canadian Multistakeholder Process on Enhancing IoT Security.

Table of Contents

Table of Contents 1

Introduction 2

Literature Review 8

Methodology 11

1. Survey 11
    1.1 Survey Development and Pilot Testing 11
    1.2 Survey Distribution 11
    1.3 Survey Limitations 12
2. Results 12
    2.1 Characteristics of Respondents 13

Findings, themes, and analysis 14

3. IoT Use 14
4. Awareness of Security and Privacy Issues 16
5. Engagement 19

Recommendations 21

6. Raise awareness and understanding 22
    6.1 Education 22
    6.2 Conversation 23
    6.3 Exploration 25
7. Enable meaningful participation 26
    7.1 Improving diversity and multistakeholderism 26
    7.2 Embed participation 27
8. Make the good way the easy way 28
    8.1 Policy changes 28
    8.2 Collaboration 30
9. Improving survey accuracy, scope, representation, and value 31

Conclusion 32

Bibliography 33

Appendix 38

Introduction

The “Internet of Things” (IoT) was coined in 1999 by Kevin Ashton. One of the founders of the original Auto-ID lab at the Massachusetts Institute of Technology (MIT), Aston introduced the term during a presentation on connecting radio-frequency identification technology to the then emerging Internet.[1] In the subsequent 2001 white paper for the Auto-ID lab, Ashton, his co-founder David L.Brock, and their colleague Sanjay Sarma, described “a world in which all electronic devices are networked and every object, whether it is physical or electronic, is electronically tagged with information pertinent to that object”.[2] Although many definitions have circulated in the last two decades, Madakam, Ramaswamy, and Tripathi offer a comprehensive and all-encompassing summary: “[IoT is] an open and comprehensive network of intelligent objects that have the capacity to auto-organize, share information, data and resources, reacting and acting in face of situations and changes in the environment”.[3]

It is important to note that contemporary understandings of IoT objects conceptually and practically differ from that of mobile connectivity objects such as smartphones, tablets, and laptops.[4] This is best illustrated through the example used in the aforementioned paper, describing IoT more specifically as when “sensors and actuators embedded in physical objects—from roadways to pacemakers—are linked through wired and wireless networks, often using the same Internet IP that connects the Internet”.[5] As such, objects which fall under the scope of IoT occupy almost every sphere imaginable — from integrated water filtration systems in food and agriculture, to security systems in household electronic items, to wearable electronic feedback gadgets like fitbits.[6] Today, IoT is one pillar of the flourishing technological ecosystem

---

[1] Ashton, Kevin. “That ‘Internet of Things’ Thing” *RFiD Journal* (2016): 1, http://www.itrco.jp/libraries/RFIDjournal-That%20Internet%20of%20Things%20Thing.pdf

[2] Sarma, Sanjay, David L. Brock, and Kevin Ashton. "The networked physical world." *Auto-ID Center White Paper MIT-AUTOID-WH-001* (2000): 4, https://pdfs.semanticscholar.org/88b4/a255082d91b3c88261976c85a24f2f92c5c3.pdf

[3] Madakam, Somayya, R. Ramaswamy, and Siddharth Tripathi. "Internet of Things (IoT): A literature review." *Journal of Computer and Communications* 3, no. 05 (2015): 165. https://file.scirp.org/pdf/JCC_2015052516013923.pdf

[4] Ibid.

[5] Ibid.

[6] Davenport, Tom, and John Lucker. "Running on data: Activity trackers and the Internet of Things." *Deloitte Review* 16 (2015). https://www2.deloitte.com/insights/us/en/deloitte-review/issue-16/internet-of-things-wearable-technology.html

with an immense capacity to continue revolutionizing human activity.[7] Youth around the world are particularly impacted due to their parallel development with this rapid-paced technological paradigm.[8]

While its capacities are novel and enchanting, little about IoT is understood by both the government and the public, save for the technologies' accelerating growth.[9] Using global sensor sales as a proxy for IoT growth, estimates indicate that IoT markets have augmented annually by approximately 70 percent since 2010.[10] By 2020, it is estimated that machine-to-machine (M2M) communications alone will generate approximately USD$900 billion in revenues.[11] In Canada, reports project the domestic IoT market will reach CAD$21 billion by 2018.[12] Globally, IoT market value is on a trajectory to be USD$1.9 trillion by 2020.[13]

The conveniences and benefits provided by IoT technologies continue to kindle their ubiquity and greater potential for economic growth. However, a primary inhibitor to the IoT sector and the potential benefits of its market tide are security concerns.[14] Currently, a pressing concern for both regulators and users alike is the potential breach of privacy exposed by IoT.[15] In a study by Hewlett Packard, 100 percent of investigated devices used in home security had significant vulnerabilities including password security, encryption, and authentication issues.[16] Additionally, the incidences of personal data breaches are increasing.[17] The *Data Breach Database* by Gemalto

---

[7] Trosow, Samuel, Lindsay Taylor, and Alexandrina Hanam. "The Internet of Things: Implications for Consumer Privacy under Canadian Law". *Policy and Research Group of the Office of the Privacy Commissioner of Canada* (2016): 1-51, https://ir.lib.uwo.ca/lawpub/91/

[8] Trosow, Taylor, and Hanam. "The Internet of Things" (2016): 1-4.

[9] Policy and Research Group of the 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" *Office of the Privacy Commissioner of Canada* (2016): 1-4, https://www.priv.gc.ca/media/1808/iot_201602_e.pdf

[10] Ibid.

[11] "Cybersecurity and the Internet of Things" *Ernst and Young* (March 2015): 1-23. https://www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-of-things/%24FILE/EY-cybersecurity-and-the-internet-of-things.pdf

[12] Masse, M and P. Beaudry. "The CRTC is not ready for the Internet of Things" *Globe and Mail* (May 22, 2017). https://www.theglobeandmail.com/report-on-business/rob-commentary/the-crtc-is-not-ready-for-the-internet-of-things/article35078149

[13] Policy and Research Group of the Office of the Privacy Commissioner of Canada. "The Internet of Things" (2016): 1-4.

[14] Trosow, Taylor, and Hanam, Alexandrina. "The Internet of Things" (2016): 16-21.

[15] Policy and Research Group of the Office of the Privacy Commissioner of Canada. "The Internet of Things" (2016): 1-4.

[16] Hewlett-Packard Development Company. "HP Study Finds Alarming Vulnerabilities with Internet of Things (IoT) Home Security Systems" *HP News* (February 10, 2015). http://www8.hp.com/us/en/hp-news/press-release.html?id=1909050

[17] "Breach Level Index" *Gemalto Inc.* (2017). http://www.breachlevelindex.com/

Incorporated identified 3,353,172,708 data records that were compromised worldwide in the first half of 2018, with a total of 13,443,149,623 since 2013.[18]

Illustrated by Maheswaran and Hashmi "[Privacy threats] can either be in the form of wrong data in the wrong entity's hands, or too much data in the hands of the right entity".[19] In other words, two thematic privacy concerns manifest: (1) authorized accumulation of user data and (2) unauthorized third party interception of such data.[20] Within these themes, four levels of security concern expose IoT users:[21]

1. Application layer (overall design of the device and program itself);
2. Computing layer (where computations occur, either in the device or on a server elsewhere);
3. Communication layer (information transport between device and servers/other devices);
4. Gadget layer (the hardware of the device itself).

The current state of affairs is ill-equipped to manage the privacy and security concerns implicated by IoT. In Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) was founded on the eight privacy guidelines recommended by the OECD as well as two other self-regulatory guidelines concerning consent and challenges.[22] According to the Office of the Privacy Commissioner of Canada (OPC), consent is considered the "cornerstone" of PIPEDA and deems knowledge and consent as prerequisites to personal data collection.[23] Obliged by PIPEDA, organizations are expected to protect collected personal data "against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification".[24] However, the law does not specify appropriate methods of data protection.[25] Thus, terms of service and privacy policies are generally lacking adequate information for consumers to assess the quality of their data protection.[26]

---

[18] Ibid.
[19] Misra, Sridipta, Muthucumaru Maheswaran & Salman Hashmi. *Security Challenges and Approaches in Internet of Things* (Switzerland: Springer International Publishing, 2017): 39-51, https://link.springer.com/book/10.1007%2F978-3-319-44230-3
[20] Ibid.
[21] Ibid.
[22] "Archived — Appendix 3: Model Code for the Protection of Personal Information" *Consumer Measures Committee* (2011). http://cmcweb.ca/eic/site/cmc-cmc.nsf/eng/fe00076.html
[23] Office of the Privacy Commission of Canada. "Consent" *Government of Canada* (2018) https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/
[24] *PIPEDA Principles Set Out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information, Statutes of Canada*, 2000, c. 5. https://laws-lois.justice.gc.ca/eng/acts/p-8.6/page-11.html
[25] Trosow, Taylor, and Hanam, Alexandrina. "The Internet of Things" (2016): 9-10.
[26] Ibid.

This report is focused on arming Canadian youth with the skills and tools to learn about IoT security. PIPEDA does not differentiate between adult and youth data.[27] However, the OPC considers youth data to be particularly sensitive and outlines non-binding recommendations regarding the collection, use, and dissemination of such data.[28]

From baby monitors to social media accounts, technological surveillance of children and youth is widespread and normalized in Western nations.[29] Given the novelty of IoT, the literature pool is limited and nascent, with few solutions and many critical questions.[30] Nonetheless, a review of research enables a better understanding of the current understanding and attitudes held by youth toward IoT, privacy, and security. When compared to older generations, youth tend to show dampened concerns about privacy in general.[31] This is most likely due to the rising ubiquity of surveillance, which leads to greater norms of data transparency.[32] However, according to the report, *Young Canadians in a Wired World, Phase III: Trends and Recommendations*, Canadian students from grades 4 to 11 are aware of privacy concerns and skeptical of external parties using their data.[33] Furthermore, this survey also showed that students were most interested in learning more about verifying online information in school, with approximately a third of students specifically wanting to learn about "how companies collect and use personal information, how to search for information online and how to use privacy settings."[34] Despite this concern, a section from the same report, *Experts or Amateurs? Gauging Young Canadians' Digital Literacy Skills*, found students of the same demographic expressed limited amounts of knowledge about the commercial aspects of their preferred online platforms.[35] More specifically, 39 percent of students incorrectly thought that companies are not interested in what they say and do online

[27] Office of the Privacy Commissioner of Canada. "Guidance for businesses that collect kids' information" (March 2017). https://www.priv.gc.ca/en/privacy-topics/privacy-and-kids/gd_bus_kids/
[28] Ibid.
[29] Research Group of the Office of the Privacy Commissioner of Canada. "Surveillance Technologies and Children" Government of Canada (October 2012): 8-9, https://www.priv.gc.ca/media/1751/opc_201210_e.pdf
[30] Ibid.
[31] Research Group of the Office of the Privacy Commissioner of Canada. "Surveillance Technologies and Children" (October 2012): 8-9. https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2012/opc_201210/
[32] Ibid.
[33] Steeves, Valerie. "Young Canadians in a Wired World, Phase III: Trends and Recommendations." Ottawa: MediaSmarts (2015): 1-14, http://mediasmarts.ca/young-canadians-wired-world-phase-iii-0
[34] Steeves, Valerie. "Young Canadians in a Wired World, Phase III: Experts or Amateurs? Gauging Young Canadians' Digital Literacy Skills." Ottawa: MediaSmarts (2015): 1-58, http://mediasmarts.ca/sites/mediasmarts/files/pdfs/publication-report/full/YCWWIII_Experts_or_Amateurs.pdf?fbclid=IwAR2_Kmf_wYWmLVnA9SOrVxAU0lcmXWyiQLjVByeL5mWuDTDV6v3K1Mz4I1M
[35] Steeves, Valerie. "Young Canadians in a Wired World, Phase III: Experts or Amateurs? Gauging Young Canadians' Digital Literacy Skills." Ottawa: MediaSmarts (2015): 1-58,

while 68 percent incorrectly thought that the presence of a privacy policy on a website indicated that the site would not share their personal information with others.[36] Thus, the want and need of Canadian youth regarding data use and privacy protection is unmet.

Although the Government of Canada has committed to addressing digital literacy among youth through various programs,[37] there are few specific and up-to-date guidelines for how to address issues of IoT security, data, and privacy.[38] The aforementioned MediaSmarts study on digital literacy among youth in Canada also noted that "the number of students who had learned digital literacy skills at school was nearly constant across grades, suggesting that these skills have not yet found a place in the curriculum and, when they are taught, occurs as a one-off rather than part of a larger digital literacy framework".[39] In fact, the existing gaps in the literature mirror the policy gap: little is understood about youth attitudes, beliefs, and behaviours towards IoT and privacy.[40] In order to build an effective IoT security policy targeting youth, the current climate must be unearthed. This report explores that climate by examining existing digital literacy pedagogies and interventions as well as youth attitudes, beliefs, and behaviours toward IoT and privacy.

Overall, while the survey conducted for this report has considerable limitations, the work is important in that it is the first of its kind. It lays the groundwork and offers recommendations for a future survey effort regarding engaging Canadians with IoT security issues – and features a lengthy discussion section on this particular area. It is our belief that policy should be backed by evidence, and thus we advocate for a large-scale, representative, and nationwide survey, building upon our findings and limitations, in order to adequately assess attitudes toward IoT and how best to engage youth in understanding its implications.

Literature Review

[36] Ibid.
[37] Steeves, Valerie. "Young Canadians in a Wired World, Phase III: Trends and Recommendations." Ottawa: MediaSmarts (2015): 1-58
[38] Hoechsmann, Michael, DeWaard, Helen."Mapping Digital Literacy Policy and Practice in the Canadian Education Landscape" (2015) http://mediasmarts.ca/sites/mediasmarts/files/publication-report/full/mapping-digital-literacy.pdf
[39] Steeves, Valerie. "Young Canadians in a Wired World, Phase III: Trends and Recommendations." Ottawa: MediaSmarts (2015): 1-58
[40] Trosow, Taylor, and Hanam, Alexandrina. "The Internet of Things" (2016): 16-21.

In congruence with the nature of IoT as an emerging technological space, the existing literature analyzing youth engagement with IoT is limited and nascent, especially with regards to educating youth on IoT and IoT issues (e.g privacy, digital literacy, security).

A 2016 survey conducted by KPMG, however, found that 31 percent of millennials (aged 18-29) have limited their use of IoT devices due to security concerns.[41] The same survey also found that 74 percent of millennials, far more so than any other age group, reported that they would be more willing to use IoT devices if they were more confident about their security.[42] This indicates that there exists an awareness of IoT privacy issues among older youths, although it is to be noted that there is yet to exist any literature analyzing the sources from which millennials and younger age groups receive information on IoT.

We also found no existing literature specifically analyzing how to educate youth on IoT and the surrounding issues. However, as IoT exists within the greater scope of rapidly emerging internet and data technologies, much can be learned from analyzing the models presented in the substantial literature on youth education in civic/democratic rights and digital literacy. Much of the literature focusing on civic and democratic education emphasizes the need for experiential, student-driven learning, both within and outside of traditional educational institutions. For example, by focusing on a research council mode, Mirra et al (2013), found that student-led research projects involving interviews, discussions with experts, and presentations, outside of traditional classroom settings, are effective in engaging youth on issues of social inquiry and critical democracy.[43] Conversely, Sager (2014) found that agency-focused pedagogical exercises within classrooms, such as mock-debate and student-led discussion, are also effective in engaging youth in thinking about issues of civic and democratic rights.[44]

On the digital literacy front, Hague and Payton (2011) discuss the insights which arise from their developing of digital literacy lessons for teachers in eight primary schools

[41] "Consumer Loss Barometer." *KPMG* (2016): 7. https://assets.kpmg/content/dam/kpmg/cn/pdf/en/2016/08/consumer-loss-barometer-v1.pdf

[42] Ibid.

[43] Mirra, Nicole, Ernest Morell, Ebony Cain, D'Artagnan Scorza, Arlene Ford. "Educating for a Critical Democracy Civic Participation Reimagined in the Council of Youth Research."*Democracy and Education Journal 21, no. 1* (2013): *1-10* https://democracyeducationjournal.org/cgi/viewcontent.cgi?article=1057&context=home

[44] Sager, Alex. "Student Designed Deliberative Forums as a Pedagogical Method". In *Civic Pedagogies in Higher Education: Teaching for Democracy in Europe, canada, and the USA (2014): 132-152.* https://link.springer.com/chapter/10.1057/9781137355591_7

and six secondary schools in Britain.[45] They found that students benefited from the incorporation of digital skills and ICT (Internet Communications Technologies) across a variety of subjects, as opposed to only within a specific "digital" subject matter.[46] They also note that although many young people are "digital natives", who have greater skills with digital technology than previous generations through extra-classroom technological interactions[47], there remains considerable space for cultivating critical digital skills in a traditional school environment, including in finding and critically thinking about digital information; differing cultural and social digital practices; effective digital communication; and safety and data privacy issues.[48] Furthermore, echoing the work of Jenkins et Al (2009)[49], Hague and Payton also note that there are uneven distributions of digital skills among youth along the lines of class, race, gender, and nationality, creating a 'participation gap'.[50]

Within the Canadian context, Hoechsmann and DeWaard (2014), in a MediaSmarts report, defined digital literacy "not [as] a technological category that describes a minimum functional level of technological skills, but rather it is the broader capacity to participate in a society that uses digital communication technology in workplaces, government, education, cultural domains, civic spaces, homes and leisure spaces."[51] The report also analyzed the framework which the government of Canada has in order to address digital literacy and digital citizenship among youth throughout the country, which involves different curricular focuses in the various Canadian provinces.[52] In Ontario, digital literacy is focused on working with ICT devices[53], particularly in business studies and language art classes[54], although the report recommends that a broader incorporation across various subjects would be more beneficial for students.[55] The curriculum also states that digital citizenship should include that "students must be made aware of issues of Internet privacy, safety, and responsible use, as well as of the

---

[45] Hague, Cassie, and Sarah Payton. "Digital literacy across the curriculum.". *Curriculum Leadership 9, no, 10* (2011): 5 https://www.nfer.ac.uk/publications/FUTL06/FUTL06.pdf
[46] Ibid, 12.
[47] Ibid, 9.
[48] Ibid, 47-49
[49] Jenkins, Henry, Ravi Purushotma, Margaret Weigel, Katie Clinton, and Alice J. Robison. "Confronting the challenges of participatory culture: Media education for the 21st century". *Mit Press* (2009): 3. https://mitpress.mit.edu/books/confronting-challenges-participatory-culture
[50] Ibid, 9.
[51] Hoechsmann, Michael, Helen DeWaard. "Mapping Digital Literacy Policy and Practice in the Canadian Education Landscape." *MediaSmarts* (2015): 4
http://mediasmarts.ca/sites/mediasmarts/files/publication-report/full/mapping-digital-literacy.pdf
[52] Ibid, 6-7.
[53] Ibid, 8.
[54] Ibid, 17.
[55] Ibid.

potential for abuse of this technology, particularly when it is used to promote hatred."[56] Regardless of the curriculum ambitions, the report also notes that Ontario's digital curriculum guidelines provide minimal defined direction for teachers and little consistency in digital literacy education.[57]

Furthermore, despite the fact that IoT devices such as "Interactive Whiteboards, Smartboards, and Promethean boards"[58] as well as "wearable devices" are increasingly used in classrooms[59], the report does not outline any need to educate youth in Canada on IoT devices and the digital citizenship issues as applied to IoT technologies. This lack of analysis on Canadian youth engagement with IoT mirrors the greater gap in the literature of youth education on IoT issues. It is also important to note that although the language of both digital literacy and digital citizenship with regards to privacy and data exist in the various provincial curricula, there exists no broader implementation strategy on these topics, let alone on IoT technology in particular. In line with the aforementioned literature on civic, democratic and digital pedagogy, however, the MediaSmarts report also emphasizes the need for experiential, student-led learning opportunities and projects, such as blogging, podcasting, social media microblogging, digital storytelling, and more, in order to facilitate greater digital understanding.[60]

In conclusion, there remains a gap in the literature with regards to youth engagement with IoT devices and the related issues of IoT data privacy, security, and digital literacy. While some youth have an awareness of privacy issues surrounding IoT, we found no data indicating how millennials have been educated on these privacy issues, and to what extent. The existing literature to be drawn from on civic education and digital literacy all indicate a need to engage students in dynamic, experiential, student-led learning, both within and outside the classroom. While there exists an admirable framework to address digital literacy and citizenship within Canada, there are no consistent educational guidelines nor any focus on the highly important and rapidly evolving IoT sphere. By surveying youth on their use of IoT devices, their level of awareness about IoT security issues, and the sources from which they receive information, our report begins to provide much-needed data and analysis. Such findings work to ensure that today's "digital natives" are not out-paced in an ever-evolving and rapidly changing global technological economy.

---

[56] Ibid, 12.
[57] Ibid, 17.
[58] Ibid, 51.
[59] Ibid, 54.
[60] Ibid, 34-40.

Methodology

1. Survey

The aim of this online survey was to provide an overview of IoT device usage by young people in the context of both at-home, and wearable use, document youth awareness of IoT security issues, and to understand how individuals in this demographic consume media. In order to achieve this, we circulated this survey through our networks, as well as through social media channels to garner responses from youth internationally. The data obtained from the survey was supplemented by insights from the 13th Internet Governance Forum, the ICANN63 Public Meeting, and the 2018 GovTech Summit.

1.1 Survey Development and Pilot Testing

The survey was developed with the intention of collecting both quantitative and qualitative responses, as we were interested in acquiring both statistical understandings and more subjective exploratory perspectives. To this end, our survey is comprised of a variety of question types including multiple choice questions, open-ended written responses, and Likert scales. To build the survey we used Google Forms, primarily for its simplicity, ease of use, and visualizations. In developing the survey, we paid careful attention to the verbiage and wording in order to minimize bias, and ensure neutrality. This involved consulting members of the Youth IGF at an IGF session, and revising aspects of the survey based on their feedback. We tried to anonymize data as much as possible so participants would feel comfortable providing truthful responses. Further, the length and time to complete the survey were carefully considered in order to ensure participants would fill it out. Overall, we settled on 13 questions, with the survey taking roughly 2-3 minutes to complete.

1.2 Survey Distribution

The survey was distributed through the networks of the researchers, including friends, colleagues, and acquaintances. Further, the survey was circulated through both the personal social media channels of researchers, as well as that of organizations such as Youth IGFs, Digital Grassroots, the Internet Society and others. Disseminating the survey via channels such as Facebook, LinkedIn, Twitter, and Instagram permitted us to reach a more diverse body of participants. Challenging conventionally accepted norms and ideas is central to the strength of their development. Gathering global

perspectives through international collaboration helps to facilitate this and strengthened the overall quality of our research.

1.3 Survey Limitations

Although distributing the survey online is relatively inexpensive, anonymous, and convenient, there are several limitations to this method. Firstly, a few questions involve participants gauging their own knowledge, and these thus rely on the honesty of the participants' introspections. As a result, these self-reports may not be accurate, and it may be difficult to confirm veracity of these responses. Although the survey does have international representation, the scope of international perspectives is somewhat limited due to the small sample size. Given that participants of this survey possess an above-average education level, findings may not be attributable to the entire population. Moreover, by nature of the survey being distributed through the networks of the researchers, it reached a relatively esoteric pool of respondents. Consequently, a much larger proportion of the young people answering this survey are likely to be informed of internet issues than a non-biased public sample. Additionally, 5% of respondents listed laptops and smartphones as amongst the IoT devices they own. Whereas these devices are indeed internet-connected, IoT devices more often refer to the connectivity of appliances which are traditionally non-internet connected. Proceeding surveys should make this distinction between IoT devices and internet-connected devices more apparent to avoid confusion. Despite these drawbacks, we believe that the survey results can nevertheless provide useful information and that more importantly, our survey and its limitations can be used to develop more adequate and comprehensive surveys that can be conducted on a much more formal, wide-ranging and representative scale in the future.

2. Results

There are estimated to be 1.2 billion youth (as defined by the United Nations) aged 15-24, accounting for one out of every six people[61]. The following analyses are based upon the 55 submitted responses from youth participants, with a roughly ±13% margin of error.

[61] "2018 World Population Data Sheet With Focus on Changing Age Structures." Population Reference Bureau. Accessed January 01, 2019. https://www.prb.org/2018-world-population-data-sheet-with-focus-on-changing-age-structures/.

2.1 Characteristics of Respondents

Characteristics are as presented in figures 1 and 2 (below).The age was reported by all participants. 49% are aged between 20-24, 43.6% are between 15-19 and 7.3% have reported their age as over 24. Also indicated by all respondents was education level. 54.5% of participants have completed their undergraduate degree, 25.5% are in the midst of completing their undergraduate degree, and the remaining have completed either their Doctoral Studies, College Degree, or work as Young Professionals. When asked to indicate their country of residence, nearly 2/3 of respondents live in Canada, with the remaining 1/3 spread between countries including India, Argentina, Hong Kong, Mongolia, Zambia, Romania, Czech Republic, and Haiti.

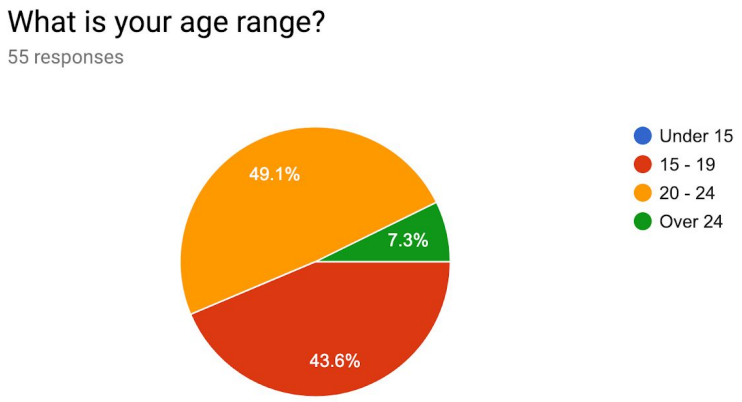

Figure 1

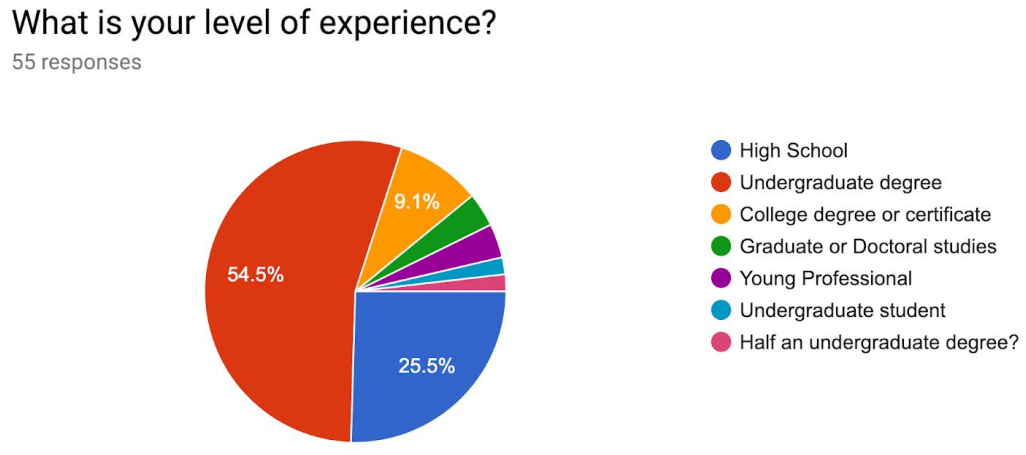

Figure 2

Findings, themes, and analysis

3. IoT Use

The survey has generated some novel insights into the use of IoT technologies by young people. Perhaps unsurprisingly, wearable devices such as smartwatches and fitness trackers (e.g. Apple Watch or Fitbit), and smart speakers (e.g. Amazon Alexa or Google Home) are the two leading IoT uses among youth (fig. 3). Several individuals stated that they interacted with multiple IoT devices, due to both their own ownership and their families' usage of IoT devices at home. However, the majority of youth do not identify themselves as frequent IoT users (fig. 4). About ⅓ considered themselves to be daily or weekly users, while nearly ⅓ stated they used it occasionally and over ⅓ of youth indicated that they 'rarely' use IoT. Interestingly, these results match those of 2017 survey by the Association of Energy Services Professionals (AESP) and Essense Partners which showed that millennials do not use IoT as much as older age groups[62].

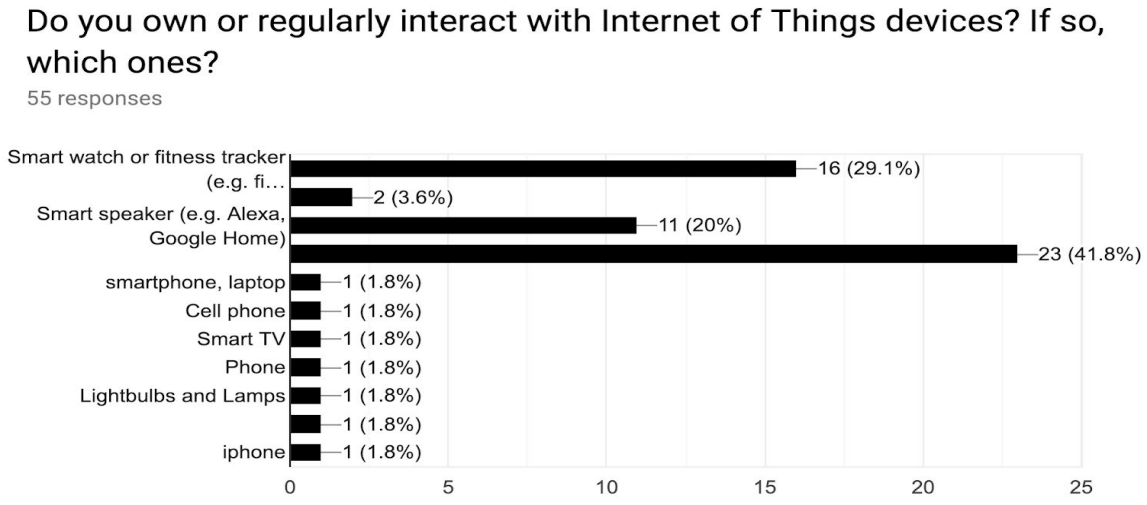

Figure 3

[62]Research, Navigant. "IoT And Millennials." Forbes. March 24, 2017. Accessed January 01, 2019. https://www.forbes.com/sites/pikeresearch/2017/03/24/iot-and-millennials/#2fab8a5e67ff

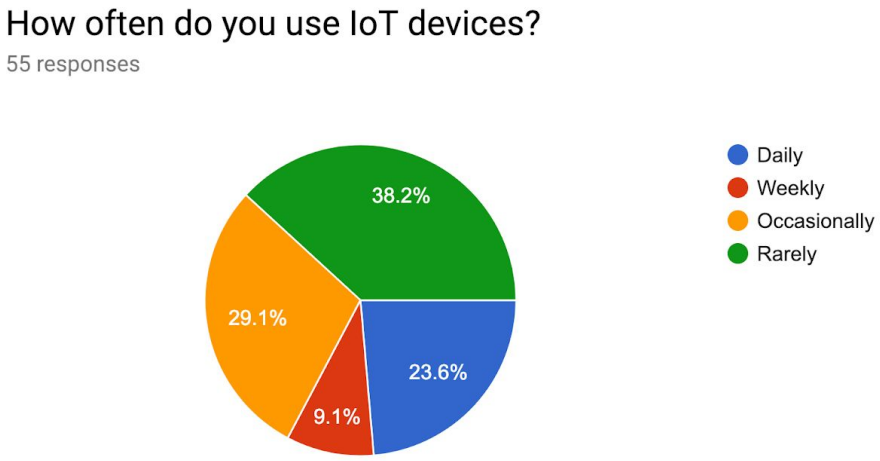

Figure 4

Overall, the participants' responses indicated a positive impression of IoT devices, specifically due to their convenience. Many comments pointed to the utility of such devices in retrieving information, and controlling aspects of the home:

"*I use my Google Home for the weather, alarms, basic questions and music. Makes certain aspects of life easier, ex. I can just ask for the weather as I walk out the door rather than searching it for myself." ; "My family uses nest as a thermostat. It's great because we can control it from our phones. (Eg. If we're out of town for the weekend we can turn it off and then bring the house back to a good temp before we return)"*

Other responses indicated the benefits of IoT in the domains of fitness and athletics:

"I use it to track my fitness. I find it encourages me to exercise more so I would say it positively effects [sic] *my life"*; *"I use a fitbit, which has encouraged me to always be aware of my physical activity. My fitbit has been a positive tool in my life; I am more focused on my health, and feel the need to ensure I reach my minimum required daily steps. It is easy to use, and ensures that I stay motivated to lead a healthier and active life."; "I'm a professional swimmer, so i track my performance, recovery and sleep with Whoop"*

Some individuals offered a more balanced view, noting that the benefits of IoT devices can sometimes be displaced by impacts to productivity:

“It makes me very efficient as I have the loT providing with the help I require but having said that it aslo [sic] *makes me dependent on a machine and reduces my own working capacity.”*

Others, however, voiced their apprehensions regarding the devices’ longevity, the social effects of these devices, and the instability of these technologies. These findings convey some awareness of the privacy and security issues regarding these devices, which will be expanded upon in the following section:

“In stores as a novelty, little to no effect”; “Less productive and less social”; “I don’t use them because I don’t trust them and it stresses me out that a lot of young people seem to not care about the massive amounts of data collected from these devices” ; My family uses Alexa more than me, I usually just ask her to play music..sometimes we unplug the device so that she cannot listen to us but frankly I'm not sure how comfortable I am with having someone record everything I say”

4. Awareness of Security and Privacy Issues

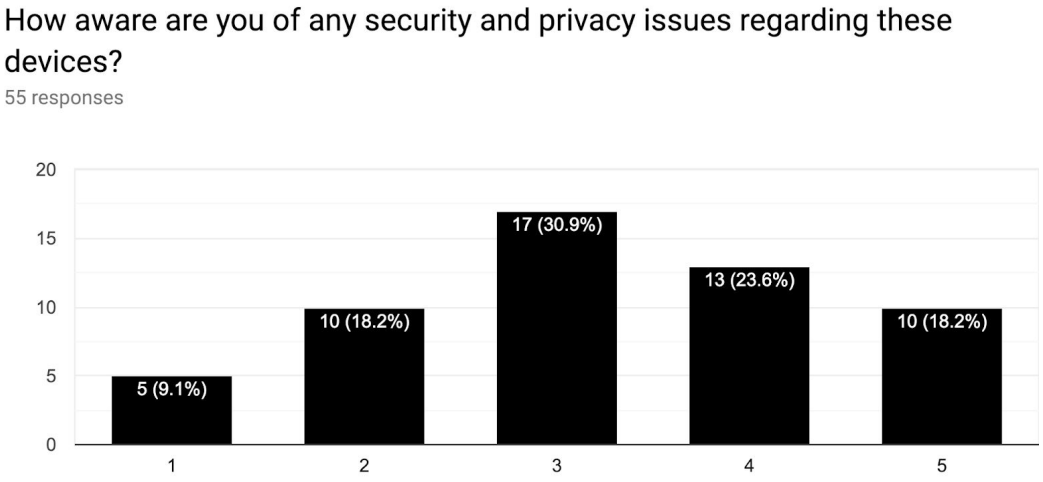

Figure 5

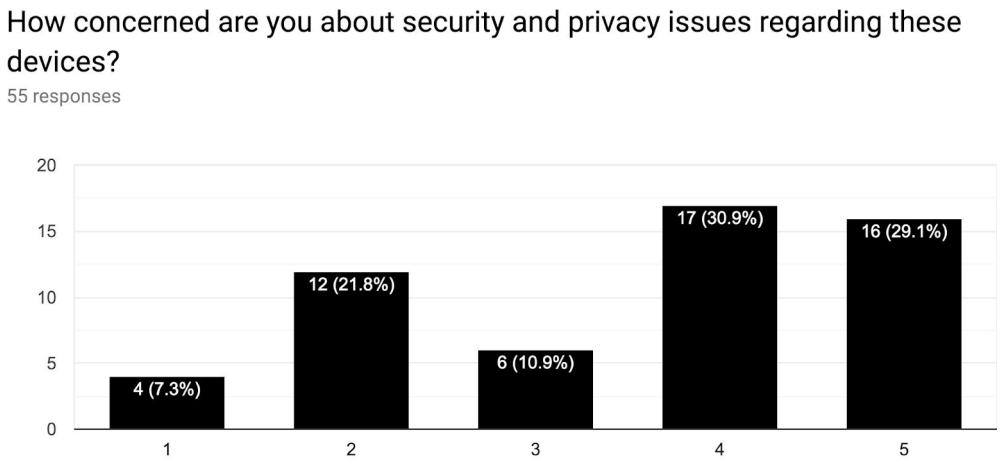

Figure 6

On a scale of one to five, with five being 'Completely Aware', the majority of respondents identified as having a mid-range (3 or 4) awareness of security and privacy issues related to IoT devices (fig. 5). But when asked to identify their level of concern, with five being 'Very Concerned', the majority indicated a higher range (4 or 5) (fig. 6). It is interesting to note how despite the benefits of IoT usage the majority of responses seem to exhibit, the attitudes towards IoT devices are decidedly more mixed. Many responses showed awareness of the security and privacy issues around these devices across a variety of contexts — specifically, surveillance and tracking, and associated data (mis)use.

Participants demonstrated a high-level awareness over the ecosystem of these devices and their functions, but admitted that they lacked specific knowledge into the technical considerations of IoT device insecurities:

"Very aware, but not so much of individual issues, if that makes sense. More just that the voice-activation that is the backbone a lot of IoT devices necessitates constant listening, which is a little unnerving. Also that Google, etc. can build user data profiles based on more "physical" aspects like voice now, as opposed to things like browsing habits. I feel like I should be more informed about this, though." ; *"Although i don't use smart devices on a regular basis, i am aware of the fact that my interaction with the device is recorded and probably analyzed for profit. I am not sure whether someone can track me down using data collected on me via smart devices."*; *"The only one I'm aware of is that they record and sell our metadata to private corporations and potentially the government."*

Others identified a lack of consumer literacy or awareness as a security issue, as well as the seemingly-commonplace breaches of personal data:

“Security consequences due to lack of knowledge from most consumers, widespread security breaches affecting data and functionality of devices that have become necessary in day to day.”; “Goverment [sic] *listening in on conversations, mics on, private information being leaked.”*

Although participants spoke favourably of the digestible, actionable insights provided to them by fitness trackers and smartwatches, participants were less enthused over the privacy implications of these devices in regards to their location-tracking capabilities:

“Location tracking can be a big problem. I'm very conscious of only wearing the smart watch on runs so it can't track me throughout the day”; “The whole idea of the device recording you and your speech and your location in the home. Very freaky” ; *“This data is stored, could be an invasion of privacy, could be used predict my behaviour It tracks location when I use it. Anyone with the information would have a good idea of where I live, maybe even the exact location.”*

However some were more indifferent towards these concerns:

“I don't really care if apple can know my gps location from my watch, I'm not hiding from anyone”

Others displayed concern over the monetization and exploitation of their personal data, specifically in the context of criminal cases and advertising:

“Smart speakers listening and recording conversations even when they’re not activated, smart speaker recordings being seized/subpoenaed by courts, abusive individuals using IoT devices to track family members/partners or restrict their movements, also generally I just don’t want private companies to have any more of my data because they will use it to try and sell me stuff or sell the data to other companies that I didn’t consent to interacting with.”; “Mass collection of personal data. Devices are always listening, any extra personal data can fall into hands of targeted ads.” ; *“Biometric data being used without informed consent, etc - listening on on* [sic] *conversations that they are not intended to listen to (GHome, Echo) - data collection, and profile building”* ; “*Listening, data mining, recording conversations, resale of consumer data (interests, questions*

etc.)" ; "Insurance companies asking for fitbit data, Alexa has recorded people's conversations and then sent it to their friends"

Some respondents also highlighted that a lack of technical infrastructure and social capacity affects security and privacy more broadly:

"I think IoT risks is currently a Western phenomena [sic]*. In global south we have other problems like internet shutdowns, lack of electricity, poor networks and so on.*"

One participant from Zambia noted that *"Internet connectivity is expensive so IoT is not sustainable. Most common IoT here is Smart TV. Smart toys exist but they are rather expensive here so are uncommon."*

5. Engagement

Much like engaging other groups, engaging youth requires not only understanding where they are most reachable but also how best to reach them. It is no surprise that engagement is now often digital by default, leveraging the reach of various platforms online to enable more widespread information dissemination and interactivity.

According to Statistics Canada, nearly 100% of youth aged 15-24 use the internet on a daily basis or own their own smartphone.[63] Within this age range, 96% also use social networking sites.[64] Given these high penetration rates, youth are often the most sought-after demographic when it comes to online marketing.

Online engagement with youth, however, can fail to account for the varying cultures which have emerged around platforms and in turn shaped their use by youth. Facebook, for example, has become far less popular among younger users in recent years. Youth now rely on Facebook mainly for its group functionalities[65], which are often the platform of choice for student groups or communities, and events. It also serves an intermediary social function, in that, given its ubiquity, powerful search function, and perceived less personal content relative to Instagram, Snapchat, Twitter or other platforms, people will often start connecting with others online over Facebook. When it comes to learning about current affairs, more than 75% of youth aged 15 to 34

[63]Statistics Canada. "A Portrait of Canadian Youth." Women and Paid Work. August 24, 2018. Accessed January 01, 2019. https://www150.statcan.gc.ca/n1/pub/11-631-x/11-631-x2018001-eng.htm
[64]Ibid.
[65]Watts, Andrew. "A Teenager's View on Social Media." Wired. June 19, 2017. Accessed January 01, 2019. https://www.wired.com/2015/01/a-teenagers-view-on-social-media/

use the internet to follow the news, over twice the rate among older Canadians.[66] According to our survey, most youths receive their news on a daily basis from Facebook, Instagram, and Twitter, in that order (fig. 7). For news sources accessed on a weekly basis, newspapers led, followed by op-eds and blogs, then other journalistic writing.

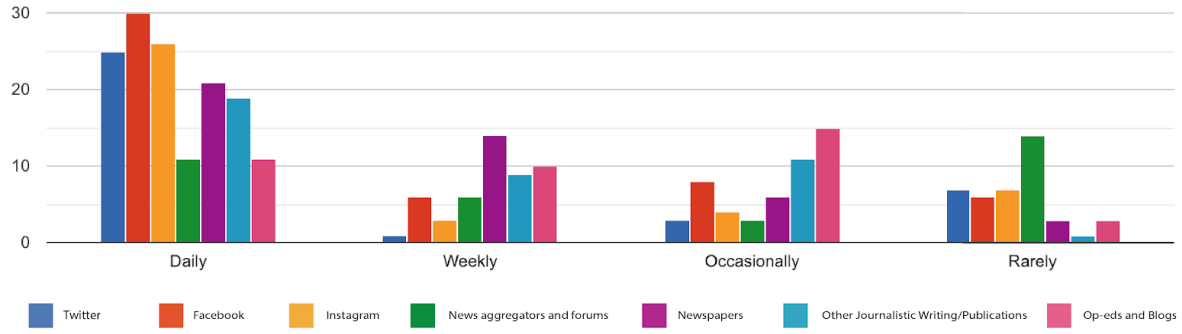

Figure 7

Given these results, it is important to consider how such platforms act as content aggregators for their users and often provide a gateway to other sources. Facebook and Twitter users are more often used to keep up to date with current events through news articles, op-eds, or discourse shared by various news services or friends, whereas Instagram users more often interact with their friends, personalities, and brands through more carefully curated visual content. Snapchat also performs a news function through its 'Discover' feed which is popular among young users and contains stories with short articles or videos from a mixture of news outlets, pop culture outlets, and celebrity personalities.

[66]Statistics Canada. "A Portrait of Canadian Youth." Women and Paid Work. August 24, 2018. Accessed January 01, 2019. https://www150.statcan.gc.ca/n1/pub/11-631-x/11-631-x2018001-eng.htm

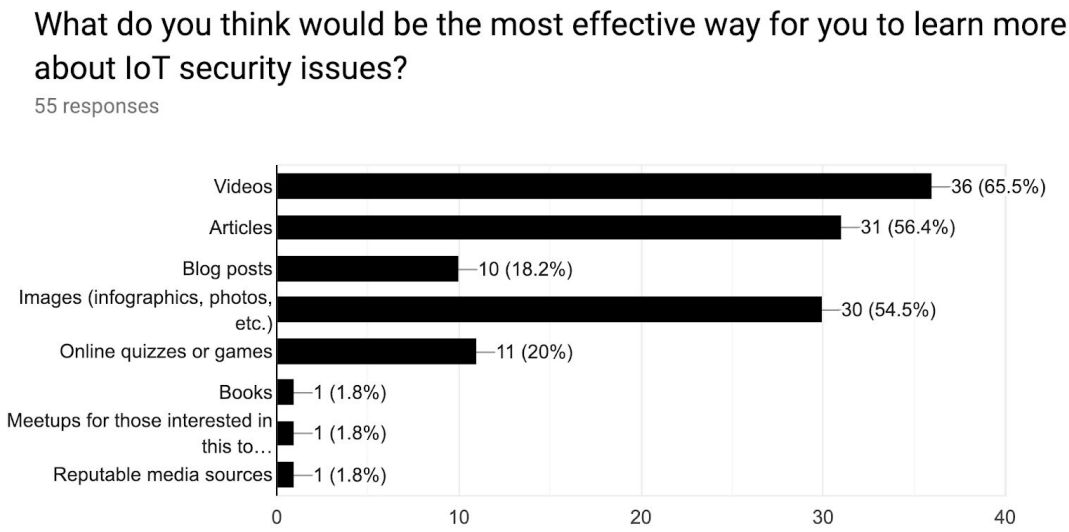

Figure 8

Increasingly governments and public agencies have prioritized leveraging these channels for public awareness campaigns directed at young people. For example, with the legalization of marijuana, Ontario's Progressive Conservative government announced that it would engage youth through a social media campaign focused on 'social responsibility'.[67] Health Canada is also exploring the use of social media influencers as part of a national vaping awareness program.[68] Interventions such as these have had mixed response, however, in the past. Youth in Ontario remember recent government and law enforcement Snapchat ad campaigns warning against fentanyl. When asked about their effectiveness, many voiced worry about whether this form of engagement could come off as 'creepy'.[69] Avoiding this reception requires matching the tone of the message to the medium or platform.

In our own research, we found that we received a larger number of survey responses after sharing the form in a more personal context (e.g. on a personal Instagram story or sending it to friends) than we did promoting it in Facebook groups or other online

[67]"Ontario Cannabis Awareness Campaign Will Target Youth: Caroline Mulroney." The Globe and Mail. October 09, 2018. Accessed January 01, 2019. https://www.theglobeandmail.com/canada/video-ontario-cannabis-awareness-campaign-will-target-youth-caroline/

[68]Dickson, Janice. "Health Canada Seeking Social Media Influencers to Warn Teens about Vaping." Thestar.com. June 16, 2018. Accessed January 01, 2019. https://www.thestar.com/news/canada/2018/06/16/health-canada-seeking-social-media-influencers-to-warn-teens-about-vaping.html

[69]Smith, Marie-Danielle. "Government Survey Confirms That, Yes, Canadian Teens Really like Their Smartphones." National Post. June 14, 2018. Accessed January 01, 2019. https://nationalpost.com/news/politics/government-survey-confirms-that-yes-canadian-teens-really-like-their-smartphones.

communities. This is in line with survey responses which showed that among those aware of security and privacy concerns related to IoT, most had learned about these issues through a combination of discussion with their personal network (e.g. friends, parents, family members, etc.) and reading articles, typically from news media. When asked what would be the most effective way to learn more about IoT security issues, most respondents recommended videos, articles, and images such as infographics, photos, or other visual representations as their preferred mediums (fig. 8).

Recommendations

6. Raise awareness and understanding

"Teens and pre-teens need to know the risks of using a digital assistant in your home and collecting all you [sic] *conversations. I don't believe the vendors who make these products are being honest about what is done with this data or who it is shared with. This includes the fact they are voice printing me and anyone who enters my home."*

Our research, though conducted on a small scale, has demonstrated that concern exceeds awareness when it comes to IoT security and privacy concerns. Young people recognize this gap and want to know more about their digital environment, specifically how it works and the true costs and benefits of using various technologies or platforms. Since much of IoT technology is still in its infancy, there is a need to educate not only young people, but society as a whole on what IoT is, how it works, what its implications might be, and how this could have an impact on our rights and interests. While "society as a whole" goes beyond the scope of our project, we believe that raising awareness and understanding must be directed toward providing all people an equal opportunity to participate by providing the necessary support different groups will require for meaningful involvement. Our project has focused on "youth", which is itself a vague and perhaps a problematic group when considering the difference in personal development between 15 and 24-year olds. Efforts toward awareness should begin far earlier than age 15; these should be combined with nascent efforts at developing such skills as digital literacy and technological competence among Canadian children. Other digitally advanced countries, like Estonia, Singapore, and Nordic countries can offer models and examples to follow through sharing best practices at an inter-governmental level.

6.1 Education

For youth especially, education policy is critical. Provincial and Federal governments should work together with civil society organizations (like the Internet Society, Media Smarts, and Code for Canada amongst others) on curricula and programs that can offer forums for discussion and awareness of IoT and other tech-related issues across Canadian educational institutions.

- ➔ **Reform curricula to better prepare students and empower them to help shape our digital future.**
  - ◆ Develop curricula that focus on improving students' digital literacy and skills including technical capabilities and their understanding of the social, cultural, political, and economic implications of digital systems from elementary school onwards.
    - At the *Youth Advocates for IoT Security* Meeting in May 2018, participants recommended working with an educational platform such as Pearson or Khan Academy to create a digital citizenship and security course which could gain accreditation and be offered online or in class across Canada with different modules for different ages/stages.
  - ◆ Improve education on civic issues and active citizenship by encouraging practical and experiential learning which teaches students how to engage with their governments and communities.
    - Develop relationships between educational institutions and their government representatives.

6.2 Conversation

One of the strengths of social media as a medium of engagement is its ability to bring people into a conversation and generate widespread interest in specific topics or events through the multiplying effects of our personal networks. Catalyzing authentic personal interest and curiosity through open dialogue which connects a specific issue like IoT security to broader social narratives or concerns is the most effective means of spreading awareness and inspiring action.

- ➔ **Conduct thorough user research to design advocacy campaigns and initiatives**

- Involve youth in determining the tone, topics, and aesthetic qualities that will resonate for certain forms of outreach. Speaking from our experience, minimalist design, mixed media, an easily navigable user interface, and concise plain language are often expected by young people in a good design.
- Adhere to inclusive design standards to ensure maximum accessibility and value for a diverse audience. Tools such as Ontario's Inclusive Design Toolkit can help here.

➔ **Focus on topics which are proven to be of interest to young people and emphasize the wider impact or interconnectedness to other areas of interest**

- Firstly, develop resources which explain the fundamentals of IoT - what is and isn't IoT, the ecology of IoT and networks, what data can IoT collect and how it does this, what data is stored and where, and how the data is used, etc.
- Place IoT issues within a broader context and demonstrate the interconnectivity and relationships between IoT and other fields, e.g.: IoT as it relates to issues in:
  - Privacy, human rights, surveillance, innovation, governance/decision making; healthcare; environment; various other monitoring and data gathering; etc.
  - Our survey results also suggest that discussions about surveillance, data (mis)use, and understanding the technical and social systems behind emerging technologies resonate with young people. Relating IoT issues to pre-existing interests of young people could prove effective and meaningful.

➔ **Consider wider issues that are factors in privacy and security**

- Survey respondents raised other concerns which they felt have not been adequately addressed in discussions about security and privacy which can take a fairly narrow perspective
  - Climate security → *"Given the current climate crisis as well as ethical concerns with the manufacture of electronics I think it's important to think about when tech can really improve something or whether we are just producing a bunch of WiFi enabled toasters."*
  - Internet access and infrastructure → *"I think IoT risks is currently a Western phenomena [sic]. In global south we have other problems like internet shutdowns, lack of electricity, poor networks and so on."*

- ◆ Recognizing and addressing these issues as part of a larger conversation on persistent inequalities and disparities in digital inclusion will help us access the full benefits of digital transformation through IoT in the long term.

➔ **Match the medium and the message**

- ◆ Find or do more user research on how youth engage with particular platforms — who or what they are following, what content are they consuming, etc. — and develop content which can be distributed through these channels or platforms that youth area already interface with
- ◆ Match tone of the message to that of the platform/medium — on platforms that have a more personalized social culture (e.g. Instagram) team up with people or groups, but be transparent in order to demonstrate that stakeholders are working with and for people
- ◆ Survey respondents suggested videos, articles, and images such as infographics, photos, or other visual representations were the most effective mediums for outreach
    - The Canadian Multistakeholder Initiative and others aiming to educate the public on IoT security or other digital issues should consider a multi-media approach which could include the following:
        - ○ Producing an article or essay series through a popular news outlet or opinion platform (e.g. Medium, Vice, etc.)
        - ○ Developing a series of short videos exploring aspects of IoT security and placing these on high impact platforms (e.g. Facebook, Twitter, Snapchat, etc.)
        - ○ Engaging social influencers to model best practices to consumers

➔ **Explore alternative forms of engagement that examine the emergence of IoT as a cultural development through creative projects**

- ◆ Support research and creative projects that look at IoT and emerging technologies in unique, artistic, and less formal ways.
    - e.g. art, performance, interactive exhibits, and other platforms which generate interest by introducing ideas in more subtle or interactive ways.
- ◆ Engage with local talent, particularly young people, to make this a reality and in doing so reach an atypical audience for what is often considered a niche policy area.
- ◆ Promoting interactivity with any creative representations to encourage sharing among people's personal networks.

6.3 Exploration

Effective engagement and capacity building will also require a deeper dive into assessing the current state of young people's interaction with digital platforms and their knowledge when it comes to not only IoT security but other topics in the tech sphere such as data and privacy rights.

- ➔ **Do further research to fill in data gaps, particularly gaining more detailed information on young Canadians' engagement online**
  - ◆ e.g. What percentage of a platform's user population are youth, how much time do they spend on each platform, what content does this age group gravitate towards, which social media accounts or other media outlets are most popular among specific age groups, what is the knowledge level of youth regarding privacy, security, and digital rights, etc.
  - ◆ This could be an opportunity to work with platforms themselves to access and make first-hand engagement data more open/transparent

7. Enable meaningful participation

Young people, in particular, are often put in the situation of being given opportunities to contribute to dialogue which feel more tokenistic than impactful. We also face constraints on our ability to participate due to busy schedules, which can prevent us from joining in on time-intensive undertakings, particularly where unpaid. Our recommendations here are intended to combat some of these challenges and explore ways to actively include an underrepresented group. The following proposals offer ways to make youth participation more meaningful, which will lead to benefits both for youth and to policymakers:

7.1 Improving diversity and multistakeholderism

Those engaging with IoT issues should be a diverse group, both themselves and regarding the organizations or groups with whom they are engaging. This will maximize the sharing and consideration of various perspectives within the IoT discussion by empowering different voices (including minority voices). There should be opportunities for such voices to make themselves heard among multiple stakeholders.

- ➔ **Diversity of age, background, and experience**

- Including various ages, backgrounds and levels of experience is an important part of promoting wider social diversity and improves the ability for outcomes to serve people equally.
- Diversity offers a different perspective – both with respect to the way in which youth engage with technologies as well as their different attitudes towards them. It also allows maximizes the involvement of all, regardless of background.

➔ **Diversity of stakeholders**

- It is important that a diverse range of groups and organizations participate in engagement opportunities, and this should not be too far skewed to certain types of organizations over others.
- The diversity of multistakeholder youth engagement should be a two-way street, meaning that youth should both engage with different stakeholders on IoT issues, and also that those different stakeholders should reach out to and offer engagement opportunities to youth, in various ways.
    - Youth should be able to engage on these issues with actors in the private sector, civil society, various levels of government, etc.

7.2 Embed participation

Avoid requiring significant amounts of additional time from young people by incorporating opportunities to learn about and engage with IoT and other emerging technologies—as well as to participate in policy making—into regular education or training activities

➔ **Improve the availability of experiential learning programs such as internships or co-op placements which provide school credit and/or compensation for work across secondary and post-secondary institutions**

- The Public Policy Forum stated in its 2016 report *The Promise and Pitfalls of the Internet of Things in Canada* that the "Government is in a position to design and execute strategic employment and investment plans related to IoT, including issues of talent and labour mobility, early education programs that emphasize math and science, secondary education programs with a focus on information technology and business and co-op programs for ICT companies and IoT-driven companies."[70]
- In Ontario, employers are incentivized to hire students through the Co-operative Education Tax Credit which provides up to $3000 to cover

[70]"The Promise and Pitfalls of the Internet of Things in Canada." Public Policy Forum. Accessed January 01, 2019. https://www.ppforum.ca/publications/the-promise-and-pitfalls-of-the-internet-of-things-in-canada/.

25-30% of expenditures incurred by each qualifying work placement.[71] BC, Manitoba, and Alberta appear to have similar schemes, but opportunities to elaborate or standardize this program should be explored across Canada.

➔ **Implementing programs and resources dedicated to encouraging and promoting youth entrepreneurship and problem-solving**

- ◆ Facilitate hackathons where young people can ideate on problems and potential applications of IoT.
  - Ensure that such events empower youth to lead proposed solutions by respecting ideas as their intellectual property and connecting them with the appropriate opportunities and resources to help with execution
- ◆ Support innovation hubs in post-secondary institutions and promote their partnership with industry, government, civil society, and others.
  - Create opportunities for younger students outside these institutions and other young people in the community to partake in hub activities and receive similar supports.

8. Make the good way the easy way

In order to transform words into action, engagement should combine the aforementioned awareness and capacity building exercises with the creation of processes, standards, and policies, in order to make compliance with best practices our default. As we operate in a rapidly evolving digital environment, these methods should be sufficiently flexible, agile, and contain mandatory checkpoints to allow change over time. Addressing the root challenges in the tech ecosystem such as data, privacy, and security can clear the path for future innovation. This section highlights areas for change that, based on the survey and secondary research, our group believes are priorities for this initiative.

8.1 Policy changes

➔ **European-style privacy laws such as the General Data Protections Regulation (GDPR) can inform and inspire the basis for regulatory and legislative approaches towards data protections reform with respect to IoT devices**

[71]Canada Revenue Agency. "Ontario Co-operative Education Tax Credit." Canada.ca. March 07, 2018. Accessed January 01, 2019. https://www.canada.ca/en/revenue-agency/services/tax/businesses/topics/corporations/provincial-territorial-corporation-tax/ontario-provincial-corporation-tax/ontario-operative-education-tax-credit.html

- With increasingly large amounts of our personal data being collected by these devices, it is imperative that their system design be premised on tenets of consent, transparency, accountability, openness, and human rights. PIPEDA and the various provincial privacy instruments must also be reviewed and reformed where appropriate to enforce these principles.
    - Companies collecting this data must clearly explain how the data is stored and used, and receive approval before collecting it.
    - Misuse of data should be subject to penalties in proportion to the severity of the situation.
    - Consent must be given in an easy-to-understand, accessible form, with a clear way for the user to grant it, and there must be an easy way for the user to revoke consent.
        - Mechanisms to foster transparency and educate consumers on device security include those created by working groups in the Canadian Multistakeholder Process on IoT Security. Once such initiative involves labelling IoT products to inform consumers of device security. Along with aiding consumers in understanding the security and privacy features of the devices, these labels serve as a means of providing suppliers with a means of displaying the product's compliance with certain standards.
    - Given that the capacity for self-regulation amongst children is limited, and that "cyberspace is a highly seductive and potentially manipulative environment for children"[72] considerations must also be made for the privacy rights of children and youth.
        - Policies should aim to consider questions such as what constitutes meaningful consent for children and youth (especially minors) and what our rights are to access, manage, remove, or modify content created on our behalf/related to ourselves considering that parents, schools, and others often capture and sometimes share vast amounts of data about us before we are adults.

➔ **Privacy by design**

- To balance the need for more data for better service design with clearly defined data rights for users, IoT devices should comply with the core

[72] Berson, Ilene R., and Michael J. Berson. "Children and their digital dossiers: Lessons in privacy rights in the digital age." *International Journal of Social Education* 21, no. 1 (2006): 135-147. https://pdfs.semanticscholar.org/7e4f/755f30b53ed115c9dd7a68892b7a7af2fb3c.pdfhttps://pdfs.semanticscholar.org/7e4f/755f30b53ed115c9dd7a68892b7a7af2fb3c.pdf

foundation of privacy by design which new regulations such as the GDPR and standards such as ISO/PC 317 aim to mandate.

- Privacy by design mandates that privacy protections be "[embedded] into the design specifications of information technologies, accountable business practices, and networked infrastructures, right from the outset" [73]. IoT devices should thus be built with data protection in mind, rather than treating it as an afterthought.

➔ **In order to create these standards and policies, it is critical to apply inclusive design methodologies.**

- Inclusive design is defined by the Ontario Digital Service as "designing for the full range of human diversity in ability, language, income, culture, gender, age, and other characteristics."[74] Designing products and services that are accessible by as many people as possible, and mandating inclusive design standards are crucial for ensuring better outcomes and more efficient policy and standards development in the long run.
- Policy approaches to inclusive design should take inspiration from the user-centred design process as defined in ISO 9241-210:2010 and involve applying more rigorous user research across the policy process before the creation of standards. Collaboration with digital government services can help enable this.

8.2 Collaboration

Internet governance involves a variety of organizations from a myriad of backgrounds. The topic of IoT security spans multiple interrelated issue areas, each of which serving as the focus of a number of these groups. In order to prevent duplication of efforts, there must be increased collaboration and harmonization between these groups at both the community and international level.

➔ **Work with ICANN, ISPs, and registrars to further the implementation of DNSSEC**

- Domain names function as a ubiquitous, scalable, decentralized communication channel for IoT infrastructure. Given that the majority of IoT applications lack comprehensive security measures, implementing

[73] Cavoukian, Ann. "Privacy by design in law, policy and practice." *A white paper for regulators, decision-makers and policy-makers* (2011). http://www.ontla.on.ca/library/repository/mon/25008/312239.pdf

[74] "Inclusive Design Toolkit." Ontario.ca. Accessed January 01, 2019. https://www.ontario.ca/page/inclusive-design-toolkit

DNSSEC can help solve this problem by securing the channel and executing application-specific security features.

- ➔ **Collaborate with digital government, infrastructure, innovation and other relevant portfolios of government to ensure adequate technical and social capacity exists for IoT uptake**
  - ◆ Align with strategic efforts related to broadband, data, and digital inclusion, as well as responses to the smart cities, debates underway
    - Many of the security, privacy, and other concerns referenced here are manifesting in ongoing discussions regarding smart cities, as they are an application where IoT, big data, AI, and other technologies coalesce with implications for citizens' navigation of virtual and physical spaces
- ➔ **Work with the ISO, other standards or assessment organizations, as well as government to develop an accreditation system for labelling based on impact assessments of platforms, products, or services**
  - ◆ The Government of Canada has developed an Algorithmic Impact Assessment which evaluates the risks of deploying an automated decision system based on business processes, data, and system design decisions. A similar tool could be developed for assessing IoT systems.
  - ◆ The B Corporation conducts Impact Assessments to certify corporations which meet high standards of social and environmental performance, transparency, and accountability. The certification promotes social consciousness and innovation by encouraging corporations to both share and compete to improve best practices. The Canadian Multistakeholder Initiative could collaborate with B Corporation and others to explore opportunities to certify IoT or tech companies based on existing B Corporation standards and new ones specifically geared toward digital technologies.

9. Improving survey accuracy, scope, representation, and value

As has been mentioned throughout this report, our quantitative results and data are significantly hampered by their small and biased sample size, as well as other important limitations (see section 1.3, page 10). However, evaluation and consideration of many of these limitations, combined with an understanding of the results and new ideas from this project, provide important first steps and design ideas for any eventual larger-scale survey to address similar IoT issues. Our report, then, can be considered something of a prototype, and it is thus important to highlight lessons learned and

areas of improvement. The following recommendation proposals build on the drawbacks of this report, as well as findings from the survey and literature review, and limitations in general:

- ➔ **Defining terms and clarifying questions more clearly**
  - ◆ Given a proportion of respondents who identified laptops, tablets and mobile phones as IoT devices with which they interacted, and given that a substantial portion of the literature on IoT excludes these devices, future surveys must be very clear on providing a proper understanding of what IoT is, together with examples and other information
  - ◆ This might be done with videos, interactive quizzes or games, or simply more detailed definitions
  - ◆ The term 'youth' should be reconsidered with an eye to whether or not this should be further separated (e.g. high school versus university/college)
    - Consideration should be given to whether younger respondents (e.g. teenagers or children) should be surveyed in another way
- ➔ **Phone-surveys to complement written/online responses**
  - ◆ While online surveys can be quick and easy, discussing questions directly–for example via phone interviews–with some portion of subjects may be of value if interested in exploring issues in more depth.
- ➔ **Achieving a larger and more representative sample, with efforts to reduce bias**
  - ◆ Any wide-ranging project, such as a nation-wide or province-wide survey effort should follow standard survey best practices including but not limited to:
    - Seeking an adequate sample size with considerations covering diversity, transparency, and consistency;
    - Discussion on whether or not random sampling is the most effective approach, and if so, how to ensure randomization;
    - Consideration of some survey inputs, such as address or postal code, to bolster reliability and verification – while ensuring responses are anonymized
- ➔ **Better coordination, and longer survey duration**
  - ◆ Engagement and coordination with different stakeholders, groups, organizations, individuals, and/or pollsters to reach out to adequate samples and numbers of respondents
  - ◆ Use a longer time period to allow for maximum responses

Conclusion

Given the scale of our study, additional research may be beneficial in helping us to better understand the best means of engaging young people in these discussions. Despite this, our report has offered valuable preliminary insights as to young people's use of and perspectives on IoT. It has illustrated both the need for engagement to increase awareness and understanding of the IoT ecosystem, in addition to providing some direction as to the desired content, tone, and medium of messaging. Further, this report has highlighted a number of concerns young people have about their security, privacy, data rights and the overall sustainability and inclusivity of emerging technologies. Finally, it has identified currents gaps in research literature and data as well as opportunities for multi-stakeholder collaboration to drive policy change.

It is our hope that these perspectives will not only support further conversation but inspire action on IoT security, particularly its impact on our collective future and how youth can contribute to shaping it. We would like to close by acknowledging that meaningfully involving youth comprises just one part of engaging in truly inclusive multistakeholderism. There is great diversity among Canadian youth and their experiences alone, and even greater diversity when we consider the range of ages, backgrounds, and abilities across all of Canada. While this report largely discusses how to engage a specific age group on a specific topic, it has demonstrated some of the disparities and varying experiences that exist among Canadians and within the world. These are essential considerations as we aim to create standards, policies, outreach campaigns, and other initiatives which will shape the way people in Canada interact with IoT. In doing so we must not only look at security and privacy but the determinants of it, because the only way to achieve a future that yields the full benefits of digitization, is to design for it.

Bibliography

"2018 World Population Data Sheet With Focus on Changing Age Structures." Population Reference Bureau. Accessed January 01, 2019. https://www.prb.org/2018-world-population-data-sheet-with-focus-on-changing-age-structures/.

“Archived — Appendix 3: Model Code for the Protection of Personal Information” *Consumer Measures Committee* (2011) http://cmcweb.ca/eic/site/cmc-cmc.nsf/eng/fe00076.html

Ashton, Kevin. “That ‘Internet of Things’ Thing” *RFiD Journal* (2016): 1, http://www.itrco.jp/libraries/RFIDjournal-That%20Internet%20of%20Things%20Thing.pdf

Berson, Ilene R., and Michael J. Berson. "Children and their digital dossiers: Lessons in privacy rights in the digital age." *International Journal of Social Education* 21, no. 1 (2006): 135-147.

“Breach Level Index” *Gemalto Inc.* (2017). http://www.breachlevelindex.com/

Canada Revenue Agency. "Ontario Co-operative Education Tax Credit." Canada.ca. March 07, 2018. Accessed January 01, 2019. https://www.canada.ca/en/revenue-agency/services/tax/businesses/topics/corporations/provincial-territorial-corporation-tax/ontario-provincial-corporation-tax/ontario-operative-education-tax-credit.html.

Cavoukian, Ann. "Privacy by design in law, policy and practice." *A white paper for regulators, decision-makers and policy-makers* (2011).

“Cybersecurity and the Internet of Things” *Ernst and Young* (March 2015): 1-23: https://www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-of-things/%24FILE/EY-cybersecurity-and-the-internet-of-things.pdf

Davenport, Tom, and John Lucker. "Running on data: Activity trackers and the Internet of Things." *Deloitte Review* 16 (2015).

https://www2.deloitte.com/insights/us/en/deloitte-review/issue-16/internet-of-things-wearable-technology.html

Dickson, Janice. "Health Canada Seeking Social Media Influencers to Warn Teens about Vaping." Thestar.com. June 16, 2018. Accessed January 01, 2019. https://www.thestar.com/news/canada/2018/06/16/health-canada-seeking-social-media-influencers-to-warn-teens-about-vaping.html.

"Inclusive Design Toolkit." Ontario.ca. Accessed January 01, 2019. https://www.ontario.ca/page/inclusive-design-toolkit.

Hague, Cassie, and Sarah Payton. “Digital Literacy across the curriculum.” *Curriculum Leadership 9, no, 10* (2011). https://www.nfer.ac.uk/publications/FUTL06/FUTL06.pdf

Hewlett Packard Development Co., “HP Study Finds Alarming Vulnerabilities with Internet of Things (IoT) Home Security Systems” *HP News.* (2015, February 10), http://www8.hp.com/us/en/hp-news/press-release.html?id=1909050

Hoechsmann, Michael, Helen DeWaard. “Mapping Digital Literacy Policy and Practice in the Canadian Education Landscape.” *MediaSmarts* (2015). http://mediasmarts.ca/sites/mediasmarts/files/publication-report/full/mapping-digital-literacy.pdf

Jenkins, Henry, Ravi Purushotma, Margaret Weigel, Katie Clinton, and Alice J. Robison. “Confronting the challenges of participatory culture: Media education for the 21st century”. *Mit Press* (2009) https://mitpress.mit.edu/books/confronting-challenges-participatory-culture

Madakam, Somayya, R. Ramaswamy, and Siddharth Tripathi. "Internet of Things (IoT): A literature review." *Journal of Computer and Communications* 3, no. 05 (2015): 165, https://file.scirp.org/pdf/JCC_2015052516013923.pdf

Masse, M and P. Beaudry. “The CRTC is not ready for the Internet of Things” *Globe and Mail* (May 22, 2017). https://www.theglobeandmail.com/report-on-business/rob-commentary/the-crtc-is-not-ready-for-the-internet-of-things/article35078149

Mirra, Nicole, Ernest Morell, Ebony Cain, D'Artagnan Scorza and Arlene Ford. "Educated for a Critical Democracy: Civic Participation Reimagined in the Council of Youth Research." *Democracy and Education Journal 21, no. 1* (2013): https://democracyeducationjournal.org/cgi/viewcontent.cgi?article=1057&context=home

Misra, S., Muthucumaru Maheswaran, and Salman Hashmi. *Security Challenges and Approaches in Internet of Things*. Switzerland: Springer International Publishing, 2017, https://link.springer.com/book/10.1007%2F978-3-319-44230-3

Office of the Privacy Commission of Canada. "Consent" *Government of Canada* (2018) https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/

Office of the Privacy Commissioner of Canada. "Guidance for businesses that collect kids' information" (March 2017). https://www.priv.gc.ca/en/privacy-topics/privacy-and-kids/gd_bus_kids/

"Ontario Cannabis Awareness Campaign Will Target Youth: Caroline Mulroney." The Globe and Mail. October 09, 2018. Accessed January 01, 2019. https://www.theglobeandmail.com/canada/video-ontario-cannabis-awareness-campaign-will-target-youth-caroline/.

PIPEDA Principles Set Out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information, Statutes of Canada, 2000, c. 5. https://laws-lois.justice.gc.ca/eng/acts/p-8.6/page-11.html

Policy and Research Group of the 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" *Office of the Privacy Commissioner of Canada* (2016): 1-23, https://www.priv.gc.ca/media/1808/iot_201602_e.pdf

Research Group of the Office of the Privacy Commissioner of Canada. **"**Surveillance Technologies and Children". Government of Canada (October 2012): 1-9, https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2012/opc_201210

Research, Navigant. "IoT And Millennials." Forbes. March 24, 2017. Accessed January 01, 2019. https://www.forbes.com/sites/pikeresearch/2017/03/24/iot-and-millennials/#2fab8a5e67ff.

Sager, Alex. “Student Designed Deliberative Forums as a Pedagogical Method”. In *Civic Pedagogies in Higher Education: Teaching for Democracy in Europe, canada, and the USA (2014): 132-152.* https://link.springer.com/chapter/10.1057/9781137355591_7

Sarma, Sanjay, David L. Brock, and Kevin Ashton. "The networked physical world." *Auto-ID Center White Paper MIT-AUTOID-WH-001* (2000): 4, https://pdfs.semanticscholar.org/88b4/a255082d91b3c88261976c85a24f2f92c5c3.pdf

Smith, Marie-Danielle. "Government Survey Confirms That, Yes, Canadian Teens Really like Their Smartphones." National Post. June 14, 2018. Accessed January 01, 2019. https://nationalpost.com/news/politics/government-survey-confirms-that-yes-canadian-teens-really-like-their-smartphones.

Statistics Canada. "A Portrait of Canadian Youth." Women and Paid Work. August 24, 2018. Accessed January 01, 2019. https://www150.statcan.gc.ca/n1/pub/11-631-x/11-631-x2018001-eng.htm.

Steeves, Valerie. “Young Canadians in a Wired World, Phase III: Experts or Amateurs? Gauging Young Canadians’ Digital Literacy Skills.” Ottawa: MediaSmarts (2015): 1-58, http://mediasmarts.ca/sites/mediasmarts/files/pdfs/publication-report/full/YCWWIII_Experts_or_Amateurs.pdf?fbclid=IwAR2_Kmf_wYWmLVnA9SOrVxAU0IcmXWyiQLjVByeL5mWuDTDV6v3K1Mz4I1M

"The Promise and Pitfalls of the Internet of Things in Canada." Public Policy Forum. Accessed January 01, 2019. https://www.ppforum.ca/publications/the-promise-and-pitfalls-of-the-internet-of-things-in-canada/.

Trosow, Samuel, Taylor, Lindsay, and Hanam, Alexandrina. “The Internet of Things: Implications for Consumer Privacy under Canadian Law”. *Policy and Research Group of the Office of the Privacy Commissioner of Canada* (2016): 1-51, https://ir.lib.uwo.ca/lawpub/91/

Watts, Andrew. "A Teenager's View on Social Media." Wired. June 19, 2017. Accessed January 01, 2019. https://www.wired.com/2015/01/a-teenagers-view-on-social-media/.

Appendix

I. Raw Data: Survey Responses

To view the survey responses, follow access to this spreadsheet.

II. Survey Response Bank

To view the analyzed data referred to throughout the report, follow access to this document.

ARJUN SANYA

Arjun Sanya co-leads Youth IGF Canada. He studies Computational Cognition with a minor in Digital Humanities and Statistics at Victoria College, University of Toronto. His interest lies at the applications of technology and design to build a more equitable tomorrow.

hello.arjunsanya@gmail.com

CAREY DAVIS

Carey is a Lester B. Pearson Scholar at Trinity College, University of Toronto. She is pursuing a double major in Cognitive Science and Pschology.

carey.davis@mail.utoronto.ca
*Twitter: @careymarin_*

JOSH GOLD

Josh Gold graduated from the University of Toronto in 2018, where his bachelor's thesis examined Estonia's strategic use of cybersecurity. He is currently working on a policy paper examining how Canada fits within fragmenting international cyberspace.

josh.gold@mail.utoronto.ca
Twitter: @joshgold3

SARAH INGLE

Sarah Ingle is founder of Youth IGF Canada. She studies International Relations, Political Science and Digital Humanities at Trinity College, University of Toronto and is passionate about the Internet, data, and human rights.

sarahmathesoningle@gmail.com
Twitter: @SarahLMIngle

ZAHIREEN TAREFDAR

Zahireen Tarefdar is a third-year undergraduate student studying International Relations at the University of Toronto. She runs an environmental policy group (@UTEAtoronto) on campus, and has research interests in sustainability, technology, global health, and information security.

zahireen.tarefdar@gmail.com
Twitter: @ZahireenT

Designed by Olivia Ingle & Arjun Sanya | January 2019