BIG DATA SURVEILLANCE: PRIVACY AND TRUST IMPLICATIONS

Date: October 21, 2021

Disclaimer: This briefing note contains the encapsulation of views presented by the speaker and does not exclusively represent the views of the Canadian Association for Security and Intelligence Studies.

KEY EVENTS

On October 21, 2021, Dr. Valerie Steeves presented *Big Data Surveillance: Privacy and Trust Implications* at the October 2021 CASIS Digital Roundtable event. This presentation was followed by a question and answer period, where CASIS Executives and attendees were given the opportunity to discuss the presentation with Dr. Steeves. The discussion topics included building an understanding of how young people view data surveillance and the strategies they have to safeguard their privacy to encourage data security professionals to design systems that enable young people to build trusting relations.

NATURE OF DISCUSSION

Presentation

Dr. Steeves argued that data surveillance by companies and social media apps rely on consent to protect young people's privacy but that this is inconsistent with young people's privacy expectations. Youth do not seek privacy by refusing to disclose but disclose and then seek to protect their privacy by controlling their audiences. Data surveillance that extracts their information, especially on highly commercialized apps and platforms, has made it more difficult for young people to interact with each other and with their parents, because it creates surveillance-type relationships where there is a lack of trust. Dr. Steeves discussed the issue of surveillance and how policies that restrict what companies can do with young people's data is needed to help young people engage with social media without the fear of being constantly monitored.

Question and Answer Period

The question and answer period primarily contained questions about how policy reform can help combat ongoing data surveillance issues involving young people and how parents can be positively involved.

BACKGROUND

Presentation

Dr. Steeves began her presentation by discussing the issues of children's safety on social media platforms. Dr. Steeves introduced three snapshots of how privacy and security policies are perceived by young people; the first snapshot discussed the gap between adults' concerns and children's concerns online. One significant example is the difference in concern regarding bullying. Children view their concerns of online bullying very differently from the way adults do, and because of this gap, adults might fail to understand that their reliance on surveillance to protect their children can sometimes have a negative impact on them. Dr. Steeves pointed out that children have developed effective strategies to combat cyberbullying but that parental fears make it more difficult to get help from adults if and when they need it.

The next two snapshots discussed protective surveillance and how it works against children. Extensive parental monitoring of children's activity on social media apps and websites hinders their ability to trust their parents. Additionally, existing policies, such as the Personal Information Protection and Electronic Documents Act (PIPEDA), do not provide reliable protection for children and their personal data as this act does not prohibit companies from forwarding their information to other institutions. This makes it difficult for children to negotiate the kinds of audience control they seek. The final snapshot involved research findings where young people argued that placing them under constant surveillance was misplaced because adults are the ones who have been behaving badly with the tones they set for their children within the online environment. Overall, according to young people, security and privacy policies have become invasive, unhelpful, out of touch, and make their lives worse. This has hit marginalized young people most, because they are often looking for a way to interact with one another within a safe space but knowing that they will get targeted by a surveillance algorithm that collects their data means they can no longer use the Internet anonymously to obtain information and participate in online communities.

Dr. Steeves then noted that young children are aware of how vulnerable the information they place online is. They are also aware that information such as gender, class, and race feeds into certain algorithms and how this information is then forwarded to big tech companies who use this information to further their economic gains. Young children also recognize the issues that persist online and how popular social media sites use their content to evoke societal expectations

through existing algorithms. Thus, policymakers should ensure that frameworks that govern young people's lives online are created in the best interest of children, not technology or corporations.

Dr. Steeves explained that big tech companies use children's information to further their commercial gain, which children are desperate to change. Dr. Steeves emphasized that children should be able to enjoy their rights, more specifically, their activity on social media without the fear of their information being extracted as a commodity.

Dr. Steeves finally noted that children want the right and power to force corporations to delete their data from corporate cloud databases. Children are also extremely concerned about the information that is being collected and stored by tech companies as it may pose a threat to their futures when they are trying to find employment later in life; they do not want an incident that occurred in their childhood to prevent them from getting a job in the future. Children are also looking for social support, which can come from a safe online community as well as parents so that they feel safe. Dr. Steeves emphasized that children are rights holders and should be able to engage online without these privacy risks.

Question and Answer Period

In the question and answer period, Dr. Steeves explained that children are at a stage in their life where they are primarily interested in communicating with friends and family and not engaging with social media in the same way that adults do. Considering that children are exposed to privacy risks online, Dr. Steeves suggested that we must analyze the way that social media sites are functioning and restrict their privacy breaching behaviours to protect children. Parental support is also important, as when children feel that they can trust their parents, issues will be handled in a less stressful manner for children.

Many children have also expressed their concern in several panel events. Thus, Dr. Steeves explained how important it is to listen to children who are openly communicating the hardships they face in the online environment, so we can help them. Although big data and tech companies believe that if information is disclosed online then it is fair to collect, use and share that information for commercial purposes, children do not agree and think that whatever information is displayed should not be commodified. Overall, the current legal frameworks that are put in place do not help children's privacy in the online realm as data companies do not follow the implemented rules. Therefore, we must start by

enforcing these rules against these companies and then reform the law so children have more protection.

KEY POINTS OF DISCUSSION

Presentation

- There is a significant gap between adults' concerns and children's concerns within the online environment.
- Parental involvement drives more frustration for children and makes the situation, such as cyberbullying, progressively worse for them to combat.
- Protective surveillance often works against children.
- Big data companies use children's private information as a commodity and for their own economic gain.
- Children recognize their rights and want surveillance restrictions for big data companies.

Question and Answer Period

- Children should be able to practice their rights and should be given an opportunity to use social media in a positive way.
- Although private information is voluntarily shared online, it should not be an opportunity for tech companies to monetize it, especially when it can pose a risk for children and their futures.
- We should analyze the behaviour of data companies and restrict the way they collect information to protect children.

Published by the Journal of Intelligence, Conflict, and Warfare and Simon Fraser University

Available from: https://jicw.org/