CROWDSTRIKE

REQUEST FOR COMMENT RESPONSE

Modernizing Privacy in Ontario

September 3, 2021

I. INTRODUCTION

In response to Ontario's request for public consultation on modernizing privacy, CrowdStrike offers the following views.

We approach these questions from the standpoint of a leading cloud-native cybersecurity provider that defends globally distributed enterprises from globally distributed threats. CrowdStrike offers insights informed by multiple practice areas: cyber threat intelligence; proactive, incident response and managed security services; and an AI-powered software-as-a-service cybersecurity platform and marketplace. Accordingly, this perspective is informed by CrowdStrike's role in protecting organizations from data breaches and a variety of other cyber threats.

II. COMMENTS

A. Rights-based approach to privacy

We agree strongly with the need for a principles-based approach to modern privacy regulations. It is critical to focus on internationally-accepted principles-based concepts rather than prescriptive technical requirements to enhance privacy while fostering technologies that secure personal data. A risk-based approach whereby factors such as the sensitivity of data in question, the impact of a breach, and mitigation actions taken by affected individuals reflects the realities of a world where technological innovation advances at a faster pace than law. This means that the nature of personal information and context of data processing activities should be central to the applicability of requirements. Consequently, principles-based approaches to data protection enable safeguards to follow sensitive data, without inhibiting technological innovation.

B. Safe use of automated decision-making

The widening adoption of Artificial Intelligence (AI)/Machine Learning (ML) periodically raises fears about automated decision-making, surveillance, algorithmic bias, and other negative externalities. In specific instances, these concerns may warrant suspicion and intense scrutiny. However, it is critical for policy makers to understand that AI/ML also has the opportunity to drive positive social outcomes; is already widely deployed in important instances driving such outcomes; and creates the opportunity for innovation in a variety of important spheres, including industries such as medicine and education.

Our comments will focus on the use of AI/ML within cybersecurity solutions. Legacy cybersecurity solutions used to rely on scanning files against signatures of previously identified malicious files. This process was onerous, resource-intensive, and could be easily circumvented through the use of novel or slightly modified approaches. Next-generation solutions, which leverage AI/ML, can detect previously unknown threats based on their characteristics or behaviors. This offers much more robust protection against threat activity.

Leveraging AI/ML can achieve success against unknown unknowns. For example, a machine learning model, shipped to CrowdStrike's Falcon Platform customers in September 2019, detected with high confidence the SUNSPOT malware, which was central to a sophisticated campaign that targeted high-value government organizations in late 2020-early 2021.[1] This is one of many instances of AI/ML typifying the best ways to defeat threat actors using new or tailored tools, tactics, techniques, or procedures.

In cybersecurity, AI is an advantage, especially when added to enterprise security solutions.[2] Cybersecurity threats are exceptionally broad, and for too long industry players have focused on narrow solutions. No box on a network or a single-purpose software agent will address the full scope of the problem. Security teams demand contextual awareness and visibility from across their entire environments,

---

[1] Sven Krasser, "Stellar Performances: How CrowdStrike Machine Learning Handles the SUNSPOT Malware," CrowdStrike Blog (Jan. 21, 2021) https://www.crowdstrike.com/blog/stellar-performances-how-crowdstrike-machine-learning-handles-the-sunspot-malware/.

[2] Michael Sentonas, *How Artificial Intelligence is Becoming a Key Weapon in the Cybersecurity War*, CrowdStrike Blog, Oct. 24, 2017, https://www.crowdstrike.com/blog/how-artificial-intelligence-is-becoming-a-key-weapon-in-the-cybersecurity-war/.

including within cloud and ephemeral environments. Indeed, with the help of AI, CrowdStrike can stop an attack in its tracks because such technology works faster than conventional signature-based or indicator of compromise (IOC)-based prevention.

We recommend that as Ontario continues to modernize privacy regulations, it keeps flexibility in mind. By this, we mean to emphasize the flexibility of AI as a positive tool in various situations, and not simply an automated-decision making system that could harm Ontarians.

We understand from the White Paper that the concern with AI is the possible harm to Ontarians, but for AI, like for any other technology, the context in which it is used, rather than the mere fact that it is incorporated, is material. Consequently,relying upon a right to object to a particular technology or data processing methodology is not the best approach to protect rights in an ever-evolving technological landscape. Instead, we recommend protecting the rights of Ontarians through a technology-neutral approach. When creating regulations on the safe use of AI, Ontario should consider adopting language similar to the General Data Protection Regulation's ("GDPR") requirement that organizations implement safeguards "appropriate" to the risk to protect personal information. This approach incentivizes organizations to take into account modern, rapidly-evolving data breach risks posed by cybersecurity threats from e-crime, 'hacktivist', and nation state actors using tactics such as ransomware, supply chain attacks, or malware-less intrusions.

C. A fair, proportionate and supportive regulatory regime

A uniform, high-level standard of cybersecurity is the best way to defend a complex enterprise. Different standards will result in unintended short-term and long-term consequences. In the short term, different rules and standards will yield divergent results, complicate security training, negatively impact the use of shared resources and services, and complicate collaboration between organizations and agencies. In the long term, independently-developed approaches will lead to confusion with respect to emerging security controls and updates to best practices. Consequently, this increases the risk of cybersecurity incidents.

This concept can be applied to a governmental regulatory scheme as well. Ontario's goal of modernizing privacy regulations should align with Bill C-11. There are frequent references throughout the White Paper to Bill C-11 and if the resulting regulatory regimes are too far apart in the end, this may inhibit the successful implementation of robust privacy protections throughout Canada on both the federal and provincial levels.

D. Support for Ontario innovators

The central challenge for governments seeking to support startups and local entrants is balancing that objective against the imperative to use validated, industry-leading solutions where they are likely to yield stronger security outcomes. While there is no formula to achieve the perfect composition of providers, a few factors focused on viability, validation, and flexibility merit consideration. First, local services providers that operate with established technology partners can bring the benefit of a mature solution augmented with local support, delivery, and integrations. Second, evaluating references from organizations with mature security programs that have successfully adopted a local technology or service can help establish whether it may be suitable for use. Finally, the establishment of an environment that's suitable for experimentation, for example, that is separate or segmented from the greater enterprise and serves less sensitive purposes, can help decision makers evaluate emerging technologies on the basis of their performance.

III. CONCLUSION

The White Paper provides a thoughtful analysis of a complex legal and policy area. The Paper demonstrates Ontario's commitment to modernizing the protection and management of privacy. As Ontario considers updating its regulations, we recommend continued engagement with international stakeholders. Adversaries innovate at a record-pace, and it's important to empower defenders to leverage global data flows, big data analytics, and machine learning to protect against ever-evolving threats. Finally, because the underlying technologies evolve faster than law and policy, we recommend and emphasize that any proposed legislative updates focus on principles rather than prescriptive requirements and include a mechanism for periodic revisions.

IV. ABOUT CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale AI and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 3 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: We stop breaches. Learn more: https://www.crowdstrike.com/.

V. CONTACT

We would welcome the opportunity to discuss these matters in more detail. Public policy inquiries should be made to:

Drew Bagley CIPP/E
VP & Counsel, Privacy and Cyber Policy

Robert Sheldon
Director, Public Policy & Strategy

Email: policy@crowdstrike.com

***