# Information Presentation Response

Considering the advances in technology and the lack of jurisdiction to regulate it, my opinion is that privacy will become more of a concern in the future given that the current system does not quickly adapt to the technology. As shown with smart cities, there are ideas floating around for products to use more and more user data to improve our lives. One might think people have been more desensitized to their data being taken, which could be true. However, I don’t believe this means it has been accepted, rather that people do not have much of a choice in the matter.

# Much Ado About Leaking

The relationship built between consumers and companies is supported solely by trust. Billions of users trust numerous companies enough to give more private information than they would give most co-workers, or at least trust enough over their competitors to be able to use their platform. I firmly believe that companies should work to provide goods for the people, and in turn can gain their trust and future patronage. I agree with Beff’s point of telling users as soon as possible, but Zark does have a reasonable point in that publishing this vulnerability online comes with some risk before they are able the patch it. It still stands that my priorities would lie in protecting the users over trying to maintain a veil of safety to mitigate, what I would consider, a small risk to the company.

Any reasonably crafted modern privacy law should dictate that companies are responsible for protecting user data from being exposed to the general public without their consent. Knowing this, Zark’s idea to hide this vulnerability from users is the exact opposite of what the users of the platform need to protect their information. As Beff pointed out, even if a hotfix could be immediately dispatched, by no means will this automatically protect all the users. A middle ground could be established here; by telling the users the security fixed after the patch has been rolled out it seems to combine the best of mitigating the risk to the company and keeping user’s privacy safe by informing them about the current risk and not drawing attention to an open vulnerability. Though it is also arguable that informing users sooner rather than later would be in the users’ best interest, as they could remove any of their data from a potential data breach before a patch can be rolled out. The main variable that could determine the greater risk is the possible damage between an active exploit without general public knowledge and an exploit after providing the knowledge to the public. I would consider consulting a security expert on that topic, but either way, the final decision should be made to build trust and protect the data of users.

On the topic of trust, it should be noted that a decision could also be influenced by stakeholders, whose main interest would be for the product to be as profitable as possible. This interest can conflict with the interests of the users wanting to protect their data from potential hackers. I would argue that building trust with users is just as important as making a profit for developing a product to be the best possible product it can be. It is not hard to imagine that a company with a clean track record of being honest, transparent, and putting its users’ interests first would gain popularity and sales because of the rarity of these traits in the capitalist version of the free market.

Keep in mind I am not an expert in computer security or business economics, so consulting the proper professionals is likely necessary for those opinions. However, from an ethical perspective, I believe any business decision needs to prioritize the general public’s interest over everything else.

# The CPPA And Internet Privacy in Canada

The general agreement is that the bill brings us closer to the standard of privacy that the United Nations lays out, but some articles argue that the standards it sets are too primitive and will actually harm the privacy of users.

A summary of CitizenLabs’ concerns is that they share critiques among other experts that the bill will not adequately address issues of meaningful consent, de-identification, or data-mobility (Kenyon, Miles). Alongside these common concerns, they also argue that organizations will not be compelled to expose their practices with users’ personal information given the current rules in the bill. Their recommendations to enhance corporate transparency are the following requirements: disclose very specifically the process in which personal data is collected and used; public transparency reports. They reason that if organizations display their practices to the users, then the users have the necessary means to control their digital personal data. An adjacent concern written is the protection of whistleblowers since the bill only states that protections only apply once the Privacy Commissioner says so. Their recommendation suggests that the whistleblower in question must be kept anonymous while the decision is still pending.

A different article by Openmedia is even more critical of the newer version of the bill, Bill C-27, saying: “If we were to give Bill C-27’s CPPA and PIDTA a grade it’d be D.” (Short, Bryan) While many of its criticisms are of the weak rules like the lower fines compared to GDPR (which is 5 years older than Bill C-27) or creating extra avenues for companies to appeal fees which delay things like class-action lawsuits. The emphasis is mostly on two other points: the fact that the bill does not talk about prioritizing user privacy over the business interests of companies, and more concretely that when compared to PIPEDA (the current privacy law in Canada), it puts the responsibility of understanding how companies use their data on the users rather than making the company responsible for properly informing them. Change of consent from comprehension to plain language they argue weakens consent and is a large step backwards.

# References

1. Kenyon, Miles. “Bill C-11 Explained.” The Citizen Lab, 12 May 2022, citizenlab.ca/2021/04/bill-c-11-explained/.
2. Short, Bryan. “The Absolute Bare Minimum: Privacy and the New Bill C-27.” OpenMedia, 14 Sept. 2022, openmedia.org/article/item/new-bill-C27#:~:text=One%20of%20the%20biggest%20misses,legislation%2C%20like%20the%20EU’s%20GDPR.