

A Defense of Privacy in the Digital Age

Justin Liu

The inexorable rise of technology has engendered a new medium for personal information to be stored and accessed. As our lives become inseparably tied to our phones, computers, and the Internet, a crucial question is whether this information should be protected. For the purposes of this paper, I define digital privacy as the right of individuals to set parameters on who can access their online information. I will argue that governments and individuals ought to defend digital privacy as a means to achieve positive freedom. To make my argument, I will begin by describing in specific terms how our information is being jeopardized and clarify that privacy should be construed as a mechanism, not an inherent end. Then, I will justify why positive freedom is valuable and the necessity of protecting digital privacy in order to preserve it. Finally, I will outline plausible steps that should be taken by governments and individuals to address this issue.

The Digital Age presents growing threats to our capacity to dictate who can see our sensitive information. Large corporations gather and distribute vast amounts of our data, mostly unregulated and unchecked. Furthermore, the revelations of Edward Snowden in 2013 illuminated the fact that the United States government is tracking virtually all of our digital activity (Mann, 2020). Canada also has similar surveillance programs, which continue to grow in scope (Petrou, 2020). Our sensitive phone conversations, emails, and text messages are increasingly susceptible to being hacked by foreign agents. Some see nothing wrong with these developments, arguing that we have no indelible right to control our information and that the

concept of privacy is merely a product of human construction. I would respond that even though privacy should not be seen as having inherent value, it does not necessarily follow that it should therefore not be promoted or preserved. This is because an entity that lacks inherent value may be a means to achieve another end that *does* have inherent value, in which case the original entity has secondary value and ought to be upheld. For example, we should eat, not because the act of eating has inherent value, but because eating is necessary to satisfy our natural human instinct to survive. The same principle applies to privacy. To determine whether it should be protected or disposed of, one must first determine the ultimate end of a just society, and then evaluate whether privacy is a means to achieve that end.

What should be the fundamental goal of a just society? The answer to this question must be rooted in an understanding of human nature. A universal human drive is the need for free and creative expression. This entails the ability to behave outside of arbitrary limiting constraints. If this is true, we ought to value freedom, and any means that promote it. Here, I must distinguish between two prevalent conceptions of freedom: positive freedom and negative freedom. The negative view of freedom says that freedom is simply the lack of direct external impediments prohibiting me from acting (Carter, 2019). For example, if I am chained to a tree, I am physically unable to move, and therefore not free. While the negative view of freedom has certain merit, I would contend that it is far too narrow. It does not include the possibility that external factors, which do not constitute obstacles *per se*, can have internal consequences, the net effect of which is still an unnatural alteration in behavior. Suppose an individual has an eccentric hobby, which he indulges in the privacy of his home. One day, he happens to see his neighbors watching him from their window. Embarrassed, he ceases to engage in this eccentric hobby. Under a strictly

negative conception of freedom, this individual is technically still “free” to engage in the eccentric hobby. After all, nobody is physically stopping him, or threatening him to stop. There are no external obstructions to his action, yet it is abundantly clear that he is not free in any practical sense. On the other hand, positive freedom says that we are free if and only if we are able to manifest our true will. I believe that from the example above and basic intuition, one can see that the positive conception of freedom is a vastly more accurate reflection of human desire and should therefore form the basis of a discussion of normative ethics. If freedom is to be viewed as something inherently valuable and worth protecting as a rational end, it must be understood positively, not negatively. It follows that a decent and just society has a moral obligation to advance positive freedom and the means by which to actualize it.

Digital privacy is a necessary condition for positive freedom. To see why, one must consider the implications of a society without digital privacy. If we are unable to set parameters on the distribution of our data, this hinders positive freedom in two major ways. First, it inevitably causes self-censoring; that is, the subconscious alterations in behavior when we perceive our information to be vulnerable. For example, an individual might be self-conscious about his digital activity, such as his intimate text messages or phone calls, entirely because of the possibility that the information could be accessed by unwelcome third parties, not just the people he intends. This precludes him from behaving in a way that reflects his true will. Second, those in positions of power can utilize our personal information in order to manipulate and sway public opinion. In 2017, it was revealed that British data marketing firm Cambridge Analytica had acquired the Facebook data of thousands of Americans during the previous US Presidential election, which was then passed on to Donald Trump’s campaign to use for political advertising

(Lapowsky, 2019). This privacy breach led to a public backlash over Facebook's lack of protection of its users' data. While Facebook CEO Mark Zuckerberg was contrite after the revelations, the Cambridge Analytica scandal evinced the deep problems with failing to uphold digital privacy. If online data can be used by political campaigns to craft advertisements and messaging, the implication is that those in power can use our own information to modify our behavior and opinions. If an individual has been subtly manipulated into undertaking an action, such as voting for a politician, can it really be said that the action is a result of free agency? Under a positive view of freedom, the answer is clearly no. If we wish to live in a free and democratic society in which we act and vote according to our authentic will rather than manufactured consent, we must have the capacity to control our digital information.

What concrete actions should individuals and governments take to protect digital privacy? Reform must start with the regulation of large tech companies. The government ought to demand that these companies encrypt their users' data, thereby ensuring that it is only accessible to those people for which it was intended. If we feel assured that our information is truly secure, we will feel less tentative and self-aware about our conduct, both online and in life more generally. Our behavior will better reflect our genuine free will. Companies should also be prohibited from sharing user data with other companies as well as the government. To be clear, I am not saying that under absolutely no circumstances should the government be able to obtain an individual's digital data. But if the government needs data from a private company to stop a prospective terrorist or criminal, it should have to procure a warrant from a legitimate court, just like the government would need to obtain a warrant to enter a house. This strikes a proper balance between respecting the privacy of law-abiding citizens while protecting the population's

safety. At an individual level, we can safeguard our digital privacy by setting complex passwords. We can also be more scrupulous about the scale of our online presence and the information we put online. But the point is that if governments regulate technology companies adequately and stop engaging in mass surveillance, we will not have to unnaturally alter our behavior out of fear of being monitored. We will be able to conduct ourselves more freely and openly like we would in the privacy of our own home.

If we wish to live in a society in which we are truly free to pursue our highest self, we must, both individually and collectively, prioritize the protection of digital privacy. If we sacrifice our information, we are essentially ceding our innate human desire for self-determination, consigning ourselves to be slaves rather than masters. As technology continues to advance, both governments and private citizens need to ensure that personal data is safeguarded in order to mitigate against the dissolution of our freedom. Only then can we build a flourishing society where we can act according to our pure will, unhindered by the forces of conformity and control.

References

- Carter, I. (2019). *Positive and Negative Liberty*. Stanford Encyclopedia of Philosophy. <https://plato.stanford.edu/entries/liberty-positive-negative/>.
- Lapowsky, I. (2019, March 17). *How Cambridge Analytica Sparked the Great Privacy Awakening*. Wired. <https://www.wired.com/story/cambridge-analytica-facebook-privacy-awakening/>.
- Mann, B. (2020, June 6). *The Biggest Leaks Revealed by Edward Snowden*. Blokt. <https://blokt.com/guides/edward-snowden-leaks>.
- Petrou, M. (2020). *Surveillance in Canada: Who are the watchers?* OpenCanada. <https://www.opencanada.org/features/surveillance-canada-who-are-watchers/>.