Smartphone Backdoors

Privacy of electronic communication has always been a contentious topic with law enforcement officers such as the police being faulted for infringing on individual privacy of citizens. Such claims have led to the question as to whether law enforcement should be allowed to use smartphone backdoors for purposes of criminal cases investigations. Johnson & Miller (2009) in *"Computer Ethics: Analyzing Information Technology"* evaluated privacy as an aspect of social good that is essential for a democratic nation and asserted that "when privacy is treated as an individual interest and then pitted against the interests of public and private organizations in a utilitarian cost-benefit framework, organizational goals and interests have trumped the interest of individuals" (p.123). In the course of such a lingering debate, some countries such as the USA have come up with the U.S. Patriot Act to empower security agencies to deal with terrorism threats by collecting data on individual citizens with less regard to their individual rights (U.S. Department of Justice, 2020). Under utilitarianism, "when a social good is balanced against the good of some individuals, social good generally wins" (Johnson & Miller, 2009, p.123). On the other hand, if two social goods are competing against each other, then they must all be considered under the ethical principle of utilitarianism. While it may be good to have individual privacy in the use of smartphones, smartphone developers should have backdoors to enable law enforcement to access encrypted information in order to avoid criminals from hiding behind digital devices.

What makes a behaviour worthwhile or not is dependent on its consequences. Johnson & Miller (2009) explained utilitarianism as "an ethical theory claiming that what makes behaviour right or wrong depends wholly on the consequences" (p.54). In applying this ethical principle, the use of backdoors into smartphones by law enforcement can be assessed. The question that goes into it is whether such an action is going to produce good consequences once it is applied. For

instance, if the backdoors are not developed to access information of an individual who has engaged in criminal behaviour, does such an action produce happiness or unhappiness? In this case, utilitarianism proposes that "actions, rules, or policies are good because of their usefulness in bringing about good consequences" (Johnson & Miller, 2009, p, 54). In this case, the involvement of law enforcement in checking out data on smartphones through backdoors is not to cause harm to the privacy but to propagate social good which is the solving of criminal acts committed through the use of such devices. Such actions are meant to have good consequences both to a democratic society and the people who have been offended through the use of such digital devices. Take an example of a person who has murdered and his actions can only be traced through a smartphone that was used to threaten or even communicate about such a crime. If the criminal's defence was that law enforcement cannot access private data, then miscarriage of justice may probably occur if the law warrants such a suspect the protection of private information at the expense of social good which in this case would be the justice to the offended.

While privacy is good for enhancing autonomy of individual behaviour as it is required in democracies, there are instances where it would be more appropriate to prefer social good to individual privacy. In explaining this end, Westin (1967) in his book, "Privacy and Freedom" argued for the case of protection of unauthorised access to individual information but adopts a balanced position that advocates against national surveillance of citizens with exception to instances when the law enforcement officers see it fit for purposes of national security. This is in line with the utilitarianism that promotes actions of every member of the society that are geared towards delivering greatest happiness to all people **(**Johnson & Miller, 2009). If the use of backdoors in smartphones would be for the purpose of infringing on privacy rights, then such an action would be actually wrong under utilitarianism. However, such backdoors are meant to

implement an investigation process for the purposes established by law as amounting to criminal investigation. In such a situation, the actions are meant to ensure that there is a common good: the society would be safer with fewer criminals. The tracking of criminal behaviour will also lead to justice in a criminal prosecution which is a positive outcome. In this case, there is balance between personal liberty and the social good because the backdoors should not be used to interfere with individual privacy, without necessarily a greater need to stop the social evil that could harm many people within a society.

Many people criticized the backdoor as "Big brother is watching you" which may lead to the spread of fear and damage to free speech. However, the idea of having watchdogs for the use of telecommunication media may also affect individual behaviour positively. For instance, Johnson & Miller (2009) described the "panoptic gaze" where prisoners were under watch by prison guards in Bentham's prison but the prisoners could not watch them back. In the "IT-configured societies, if much of what we do is recorded and likely to have future consequences, in the way we are treated, then we have to consider our watchers and their norms whenever we are watched" (Johnson & Miller, 2009, p.124). This idea is relevant in the case where the police have to act for the purpose of law enforcement because people will adopt positive behaviour in anticipation of legal consequences if they use smartphones to perpetrate or facilitate crimes. In essence, the misuse of telecommunication devices is a practice that should not be tolerated in a society and allowing backdoors for law enforcement is not so evil after all.

The smartphone backdoors might be used to investigate a case of personal privacy breach propagated by criminals who are propagating social evil rather than social good. In "*Computer Ethics and Society*," Ermann & Shauf (2003) argued that technology is not neutral and can be used to conduct what can be characterized as criminal activities ranging from unauthorised access to

personal information to "receiving junk mail or harassing phone calls" (p.151). In such a case, an individual will not be enjoying the autonomy which is considered to be a social good in a democracy. The alternative will be to engage security agencies to determine who caused such criminal violations of private intrusion. The backdoors will thus be helpful in combating such kind of information by allowing law enforcement officers to discover who was behind such criminal acts. The PIPEDA principles also allow access to private information by a law enforcement agency for the purpose that might be deemed appropriate under the law (Office of the Privacy Commissioner of Canada, 2020). This would promote the common social good for all members of the society as advocated for by utilitarianism.

In conclusion, this essay has supported the argument that it will be important for the smartphone manufacturers to allow law enforcement officers backdoors access to encrypted information when investigating criminal activities. This is based on utilitarianism that supports that an individual action should promote social good for all other members of the society and cause happiness as opposed to unhappiness. Legal enforcement can also use backdoors to smartphones encryption to investigate criminals who access peoples' private information without their consent. However, such access should not be used by legal and state agencies to promote their own selfish institutional interests against those of the citizens because that would not translate to the common social good that utilitarianism seeks to promote. The PIPEDA principles also allow for the access of private information as guided by the law and this shows that authorized access to private information by law enforcement officers under an environment controlled by the law is more likely to promote social good which is desired in any democracy than cause privacy infringement.

Word Count: 1290

References

Ermann, M. D., & Shauf, M. S. (2003). *Computers, ethics, and society* (3rd ed.). Oxford University Press, Inc.

Johnson, G. D., & Miller, W. K. (2009). *Computer Ethics: Analyzing Information Technology* (4th ed.). Pearson Education International.

Office of the Privacy Commissioner of Canada (2020). *PIPEDA fair information principles*. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/.

U.S. Department of Justice. (2020). Life and Liberty Archive. Justice.gov. Retrieved from https://www.justice.gov/archive/ll/archive.htm.

Westin, A. (1967). Privacy and freedom. *Washington and Lee Law Review*, *25*(1), 166.