[Name of the Writer]

[Name of Instructor]

[Subject]

[Date]

Research Portfolio Entry #1

Work Cited

Bennett, Collin J*. Resisting the Spread of Surveillance*. Institute of Technology, 2008

Rhetorical Precis

In the book, “Resisting the Spread of Surveillance," written by Collin J. Bennett, analyses the people and groups who are aimed at challenging the increasing inclusive ways through which personal information is processed, captured and disseminated. The author described a network of privacy advocated that are self-identified and emerged from civil society with a fewer resource without official sanctions. (Bennett, 2008). Privacy and surveillance are examined from the perspective of independent activists who have chalked out creative ways that can affect both practice and policy. The author examines that there is a frame of issues, aiming at the code of conduct and strategies that are used by both corporations and governments. The author analyzed and presented a series of case studies that can illustrate the efficiency of the efforts including conflicts over key-escrow. Bennett illustrated how loose coalitions of any private network could develop into a better, cohesive and international social movement. The author brought an in-depth analysis by conducting semi-structured interviews with more than thirty advocated around the globe and took a review of archival data, inferring that privacy is a social problem that needs to be catered at the very first edge of intersection between the groups of advocate through loosely connected networks.

Evaluation

“The Privacy Advocates: Resisting the spread of Surveillance” is written by Colin J. Bennett who is serving as a professor of political science at the University of Victoria. The book was published by MIT Press in 2008. MIT Press is a university press that is affiliated with the Massachusetts Institute of Technology. As the author has expert knowledge of political science, it can be inferred that the book is a complete code that can intimate the stance of privacy advocates and their efficiencies regarding privacy. In the book, “Resisting the spread of surveillance", the author has brought into insight the framework of "privacy advocates." There is a detailed account of history that has made privacy advocates spring from different areas of civil society. The author displayed dark practice of advocacy and privacy where computers are a source of mass surveillance and privacy. (Bennet, 2008). Bennett has classified the groups into privacy related issues termed as privacy-centric groups, privacy explicit groups, and privacy marginal groups. It is critical to note that the author has highlighted a self-narrated tale to evaluate the trajectory of advocates in the future. Bennett created a difference between the notion addressing privacy concerns and the present time, adhering to the fact that there are a variety of ways through which personal information is disseminated, captured and processed. Author inferred a picture that is an amalgamation of modernism and the trends towards privacy that are embellishing from appearance but pathetic in terms of application. It would not be wrong to say that the book is a collection of empirical evidence that addresses the theoretical frameworks of different areas such as network governance theory and policy studies. (Bennet, 2008). Bennett has lamented the struggle against the intrusive surveillance by giving readers an insight into the organization of activities by the advocates after coordinating them with an advocate’s struggles. It would not be wrong to say that the author has intimated a number of features that are beyond the understanding of policy studies and its interference in privacy.

Note # 1

Colin J. Bennet has made an analysis of the people and groups who have emerged in order to challenge the intrusive ways employed to process, capture and disseminate personal information. The book is a detailed account of the fact that the world is like a shell in which information is stored and protected with an apparently well-suited procedure with an underlying stance of disturbed technologies. (Bennet, 2008). There is an analysis of surveillance and privacy not from the technical, legal and political perspective but from the perspective of independent activists who have inferred creative ways to affect the practice and policy side by side. **Summary**

Note # 2

But globalization on its own does not create transnational movements: after two decades of the development of the Internet, in 2001, there was not yet a sustained and unified transnational privacy movement. (302). **Direct Quote**

Note # 3

The author has exhibited a framework that can narrate the ground basis of the “spread of surevlienece” taking into account that there is a continuous fight for privacy in the digital world. There is an extensive relationship between the data authorities and the advocates who are struggling to manage in the realms of digital gadget (301). **Paraphrase**

Note # 4

Bennett argued the notion of privacy advocates, taking into account that privacy advocates are trying to transform their work into a social movement paralleling to the environmental movement. Although there is a great struggle to address the stance since there is a gap in the testimony of advocates who can address a reaction to ideological privacy and security stance. (108) **Paraphrase**

Note # 5

The author has shared the background of data resilience by adhering to the idea of data spills as one of the unique and novel ways for formulating the data breaches. He quoted the example of oil spills, targeted by the environmentalists considering them destructive to the human environment. In the same stance, there is a parallel relationship between advocacy literature and advocacy experts, addressing privacy. (115) **Paraphrase**

Research Portfolio Entry # 2

Ding, Guo, et al. An Amateur Drone Surveillance System Based on the Cognitive Internet of Things. IEEE Communications Magazine, vol. 56, no. 1, Jan. 2018, pp. 29–35. Business Source Elite.

Rhetorical Precise

Drones, an aerial vehicle that is also known as "mini-unnamed aerial vehicle" is one of the famous gadgets of the present time that has attained a lot of attention due to the ample implication in all the field of daily life such as communication, public services, agriculture, surveillance, and photography. It would not be wrong to say that the deployment of amateur drones have posed certain and potent privacy, safety and security threats as well. In order to address these challenges, there is great attention towards the amateur drone surveillance adhering to the fact despite potent threat, there is much less discussion. (Ding, et, al. 2018, pp. 29–35). The author has proposed a version named as Dragnet that aims at the tailoring of emerging cognitive internet of the art framework taking into account the analysis of amateur drone surveillance. Anti-drone technologies are imparted to analyses the stance of existing studies that can be categorized into four major classes such as, mitigation techniques, warning techniques, jamming techniques, and spoofing techniques. It would not be wrong to say that the author has incorporated a stance of characteristics that can be implemented to adhere to security techniques such as detection, localization, and tracking accompanied by control and other safety techniques.

Evaluation

A collection of six authors have written an article, “An amateur Drone Surveillance System Based on the Cognitive Internet Things." All the authors are affiliated with the field of communication and engineering with a profound research background. The expertise of the authors highlights the validity of the work and research done. The article was published in IEEE Communication magazines in 2018. IEEE communication magazine is an award-winning magazine that aims at the publishing of international coverage of issues and advances that are associated with the communication. In accordance with the review published on Jstor, the author has profoundly narrated the stance of evaluation of the security concerns associated with a drone, taking into account its massive implication in all the fields of life. The author has argued the recent and past security implications in terms of safety regarding drones. (Ding, et, al. 2018, pp. 29–35). The author has inferred a brief survey that can show the state-of-the-art studies related to amateur drone surveillance. The survey is preceded by the “vision" portrayed by the author in order to address the recent emerging cognitive internet things. The author has inferred certain strategical techniques that can be used to cater to the privacy concerns associated with the drone. It is significant to note that the author has also incorporated the technical challenges and open issues that are to be faced by providing a case study on the classification and authorization of the amateur drones. In a nutshell, the article is a fruitful research that addressed a single paradigm of privacy concerns taking into account that extensive research interest. It is significant to note that the authors have made use of both objective and subjective data in order to enhance and clarify the stance of research. (Ding, et, al. 2018, pp. 29–35).

Note # 1

“An Amateur Drone Surveillance System Based on the Cognitive Internet of Things” is an account that paves the way for the analysis of the modernization in terms of privacy and security taking into account that the authors have directed the matter of discussion to an unaddressed topic. Although present is accompanied by a versatile discussion on the use of the drone, still there is much less attention given to the privacy concerns that are associated with it. The authors have not only highlighted security and privacy threats, but there is a detailed analysis of the techniques that can act as a tool against the stance of security threats. The inclusion of a case study has brought a practical implication of the mentioned techniques. **Summary**

Note # 2

Generally, machines (e.g., cameras, sensors, radars) have relatively high surveillance accuracy, but the number of them is limited. A large crowd of people can contribute surveillance data in the way, for example, mobile crowd sensing where individuals with sensing and computing devices (such as smartphones, in-vehicle sensors) collectively share data and extract information to measure and map phenomena on the presence of any amateur drone. **Direct Quote**

Note # 3

FAA has published about more than 200 facility maps that have the potential to streamline the authorization process of a drone. (Ding, et, al. 2018, pp. 29–35). These facility maps were published from 27 April 2017 taking into account the aim. i.e., to streamline the stance of authorization of drones. Even in the present time, the FAA is coordinating with the industry and the government partners to infer technologies that can be used to detect drones within the realms of airports. **Paraphrase**

Note # 4

Although a lot of work has been done to bring into consideration a variety of individual devices or the other systems that can see, sense and analyses the physical world of drone surveillance, it is significant to note that the aim of such devices is to ensure the fusion of information by addressing the research trend. **Paraphrase**

Note # 5

The internet of things is a technological revolution that has the potential to bring new connectivity, communication, and computing era. In the last few decades, there is a complete stance of worldwide efforts that can infer the development of IoT from the academic community. It is significant that a major portion of technology is concerned with computing, communication, connectivity, and control. **Paraphrase**

Research Portfolio Entry # 3

Macnish, Kevin. Government Surveillance and Why Defining Privacy Matters in a Post‐Snowden World. Journal of Applied Philosophy, vol. 35, no. 2, May 2018, pp. 417–432.

Rhetorical Precise

Kevin Macnish, author of “Government Surveillance and Why Defining Privacy Matters in a Post-Snowden World” has brought into insight a framework that refers to the long-running debate stressing either privacy is a matter of access or control. It would not be wrong to say that the framework of privacy is something to consider. The debate has been analyzed by the inference of vast collection of data that is transferred from the internet through signal intelligence agencies such as NSA and GCHO. (Macnish, 2018, pp. 417–432). The author implies that

The control of privacy is more like a mistake because there is no problem in seizing control of the personal information. It would not be wrong to say that the debate surrounds government surveillance of internet communication, taking into account the fact that privacy is all about accessing rather than controlling. There are certain harms in the actual loss of privacy, inferring the measure of access. In a nutshell, it has been brought into insight that there is access to private information by the automatic system as well as by human, referring to the violation of privacy. It would not be wrong to say that there is a gross violation of privacy by involving all data that was searched and brought into facts associated and accessed by human analysts. (Macnish, 2018, pp. 417–432).

Evaluation

I read a review that was published on Semantic Scholar, in which there was an analysis of the article. The review highlighted that it was 2013 when Edward Snowden aimed at handling over the thousands of classified documents to the reporters who had launched a firestorm of criticism taking into account both US National Security Agency and the author. The incident highlighted the underlying features of security as a necessity or just a concern. (Macnish, 2018, pp. 417–432). Kevin has argued that there are two sides of the argument, at one side is the stressing group, according to whom loss of control over one ‘s information refers to the loss of privacy while the other aspect highlights that the loss of privacy is actually a stance in which the information of an entity is actually accessed. It would not be wrong to say that the two sides are opposing to each other, inferring that there are no significant aspects that can define privacy, while control is something that is either not necessary or not sufficient for privacy. The Snowden revelation has highlighted that “privacy” is all about access and this access is carried out by a human being. The author asserts that the swathes of data collection are investigated by the automated systems that are in search of certain keywords and phrases. If the access to data is considered as the violation of privacy, then there has been a gross violation of privacy adhering to both human access and search by an automated system. (Macnish, 2018, pp. 417–432).

Note # 1

Government Surveillance and Why Defining Privacy Matters in a Post-Snowden World is more like a debate that questions either privacy is a matter of access or control. The author has highlighted two opposing sides of the same argument. In a nutshell, the arguments highlights that control account of privacy are mistaken, however, the consequences are also variant. There are two paradigms associated with control account; the first reason highlights the loss of control over information increases the risk of access to information while the other aspect highlights that loss of control over information increase the risk of privacy are violated. **Summary**

Note # 2

If I am correct in defending the access account of privacy, then arguments about privacy are a red herring: focusing on privacy distracts all involved from the real issues of harm to the general populace. Indeed, by focusing the argument on privacy, it may be harder to persuade supporters of actions taken by NSA and GCHQ that what they are doing is harmful. **Direct quote**

Note # 3

Inness has argued that privacy is not a neutral concept; in fact it is a description of access to the account. Privacy is not a good simplicter as it enables the people to do things that are not expected of a moral human being. There is a conflate that questions the value of privacy taking into account the value of actions performed under privacy concerns. **Paraphrase**

Note # 4

The author has inferred that either privacy is something that is tarnished by sharing. It has been brought into insight that humans are intact with the degree of intimacy, acting as a tool to define a relationship. (Macnish, 2018, pp. 417–432). In such a stance, privacy demands a surrender or enclosure. It is asserted that privacy is an abstract that is lost and gained at the same time, sharing information will lose the privacy but it will infer intimacy taking into account the stance of a stronger degree of relationship. **Paraphrase**

Note # 5

The author has defined privacy control as a recession in rights and interests that are protected by privacy concerns. It would not be wrong to say that loss of privacy is a stance that highlights the facts associated with loss of security and adherence to the tool of fear that can incorporate the control on information. Invasion into privacy is not only a threat; in fact, it is a tool that can hamper the entire special spectrum associated with an individual. **Paraphrase**

Work Cited

#### *Altmetric – Government Surveillance and Why Defining Privacy Matters in a Post-Snowden World*. (2019). *Altmetric.com*. Retrieved, from https://www.altmetric.com/details/7877321

Bennet, Collin J*. Resisting the Spread of Surveillance*. Institute of Technology, 2008

Ding, Guo, et al. An Amateur Drone Surveillance System Based on the Cognitive Internet of Things. IEEE Communications Magazine, vol. 56, no. 1, Jan. 2018, pp. 29–35. Business Source Elite.

#### Macnish, K. (2016). Government Surveillance and Why Defining Privacy Matters in a Post-Snowden World. *Journal Of Applied Philosophy*, *35*(2), 417-432. doi:10.1111/japp.12219

*SAGE Journals: Your gateway to world-class journal research*. (2019). *Journals.sagepub.com*. Retrieved from <https://journals.sagepub.com/doi/abs/10.2189/asqu.2009.54.2.334>