**SCHOLEDGE International Journal of Management & Development**
ISSN 2394-3378, Vol.06, Issue 5 (2019)
Pg 67-70.
Paper URL: link.thescholedge.org/1055

Published by: SCHOLEDGE Publishing
www.theSCHOLEDGE.org
Email: editorial@thescholedge.org


# A Contemporary Analysis of Online Privacy & Data Protection in the context of Parallel Privacy Policies

**Rita Kaul**
Founder, Freelancer & Edtech Management Coach
Alumnus, The University of British Columbia, Vancouver, Canada.

We are living in an age where we exist less offline but mostly online. Most of our records and data are shared online whether privately or publicly. A part of this data is posted by us ourselves and a part is kept in digital form by our service providers, insurance companies, banks, governmental agencies and others with whom we have formal relations of any kind. When most of our data is available online whether privately or publicly, we need to be cautious about where to share our data and to know how our data is kept safe. This article is all about our online presence, our data and its privacy & protection. This article analyses how successful we are in keeping our online presence by following those 'privacy policies' which we most of the time don't take time to read before accepting to use any online service.

**Keywords**: Online Privacy, Data Protection, GDPR, Online Hygiene, Web Security

Following many model practices and some mandatory regulations like EU GDPR (European Union- General Data Protection Regulation), most of the modern-day websites (if not all) are having a 'privacy policy' in some form or the other. Some call it privacy policy while some may term it data protection policy or terms or use.

**What These 'Privacy Policies' are All About?**

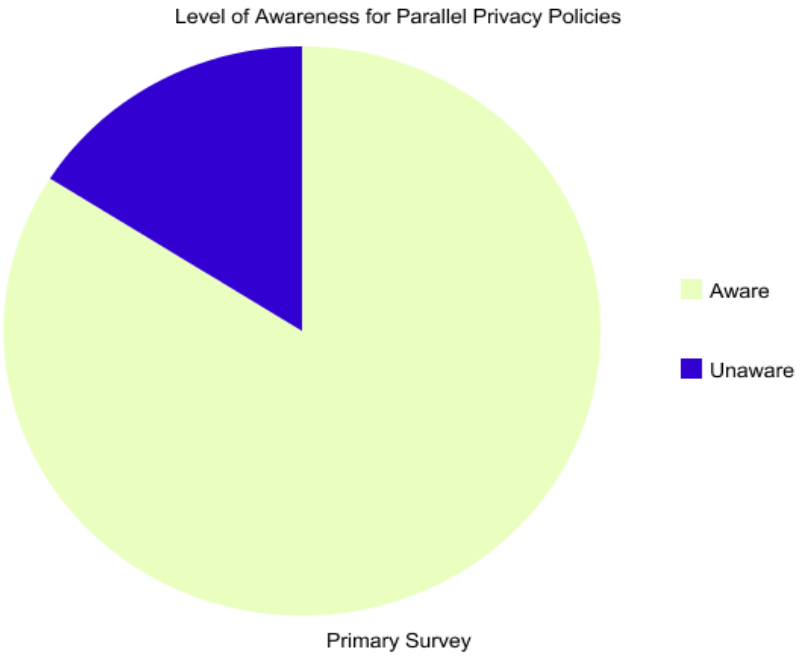
These privacy policies mention how your data will be used by those websites if you start using them by creating or entering your personal data i.e. email address, residential address or phone number etc. These privacy policies following the applicability of the EU GDPR also mention how your data will be used by these websites, how the data will be kept safely, how the same will be transmitted or processed. These policies also provide

how and when you will be notified if there were any compromises on the part of these websites having your personal data.

**Parallel Privacy Policies: The Real Thing We Often Overlook?**

Nowadays, businesses (mostly online ones) have other online businesses in tie-ups overdoing something in collaboration to provide you with the services or merchandise. These privacy policies also mention if your personal data will be shared with these partners of them. Most of us do accept those circumstances and agree with the mentioned privacy policy to continue using that particular web service/website.

What we overlook is the fact that those partners of the website whose privacy policy you just have accepted, also do have their privacy policies (these are called as 'parallel privacy policies') which further govern the data handling including the data which they use to get from the websites which you have just started to use. Your data is flowing to the websites where you directly entered into and to the websites which you didn't agree to.




The primary survey conducted via LinkedIn platform has found that the only 84% of the survey population of 129 persons weren't aware of the parallel privacy policies whereas only 16% were aware of what we call the parallel privacy policies. The survey has also found that none of the survey population was concerned about agreeing to the parallel privacy policies. The survey finds that the parallel policies in the absence of an express agreement of the end-users may mishandle their data without information of the end-users.

**Parallel Privacy Policies: How Does it Affect You?**

Almost every one of us does receive random emails from the sources or companies to whom we never passed our email addresses. Wondering from where they get your email address? They get your email address including your other information which is being circulated over the web by and between those websites you at one time or the other agreed to use. It is that covenant of the privacy policy of those partner websites which weren't agreed to by you expressly but you have done the same impliedly (though involuntarily).

This way, you and your online presence along with your data become a commodity, a digital commodity which is a valuable asset but you aren't paid for the same. Your online presence is being traded over the web without your knowledge or agreement.

**Parallel Privacy Policies: Whose Accountability to Protect Data?**

Various privacy legislation enactments have just started to take place which has necessitated for ensuring the accountability for the data handling and its protection. The Facebook–Cambridge Analytica case can be seen as a perfect example of the failure of Facebook to ensure to have a look at the parallel privacy policy of Cambridge Analytica.

The primary responsibility for the protection of your data is that website to which you primarily entered your data. In case of any compromise whether on part of this particular website or on part of its collaborating partners, you are a grieved party to that primary website.

But, it doesn't mean that you shouldn't question the privacy policies of the website's partner websites. In case you come to know of the instance when or where your data can inappropriately be used by those partner website, you can very well ask the website operator to have an attention to the parallel privacy policies of their partner websites.

Now comes how the business should play their role. The businesses should also have an updated record of the privacy policies of their partner businesses with whom you are bound to share data of your users to fulfil your commercial commitments. The businesses must point out any conflict leading instance which can otherwise be very well avoided by making an amendment or update in the privacy policies of the partner websites. The businesses should also ensure that these parallel privacy policies comply with the industry model norms as well as the regulatory norms to avoid any instance of criticism on data protection front.

**Exclusive Data Usage Clause in Parallel Privacy Policies: Need of Hour**

The online businesses should ensure that the data which will be shared by them to their collaborators or partners must be used for the intended purpose of fulfilling their commitments with the websites in the first place and must be deleted after the purpose is concluded unless it is an ongoing service arrangement.

The privacy policies must mention that the data from the partners will be used for the purpose for which the data will be acquired and not for any follow-on transmission to any third party or without the express permission of the primary holders (primary websites) if there is a mention in the privacy policies of these primary websites (which the primary users agreed to in the very first place.)

**Conclusion**

It can very well be concluded that the privacy policies and the parallel policies all are for the attention and agreement of the end-users of any web service. Hence, the end-users need to be very well served with transparent privacy policies (primary as well as parallel). This will boost confidence in the end-users where they feel that they, their online presence and their data is being protected and handled cautiously.

**References**


[1]. Buchanan, T., Paine, C., Joinson, A. N., & Reips, U. D. (2007). Development of measures of online privacy concern and protection for use on the Internet. Journal of the American Society for Information Science and Technology, 58(2), 157-165.

[2]. Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. Journal of computer-mediated communication, 15(1), 83-108.

[3]. Milne, G. R., Rohm, A. J., & Bahl, S. (2004). Consumers' protection of online privacy and identity. Journal of Consumer Affairs, 38(2), 217-232.

[4]. Pollach, I. (2007). What's wrong with online privacy policies?. Communications of the ACM, 50(9), 103-108.

[5]. Wu, K. W., Huang, S. Y., Yen, D. C., & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. Computers in human behavior, 28(3), 889-897.

[6]. Yao, M. Z., Rice, R. E., & Wallis, K. (2007). Predicting user concerns about online privacy. Journal of the American Society for Information Science and Technology, 58(5), 710-722.