Hyper-Connected Information Architecture and Users' Privacy Protection

Sohaib Khawaja

Syracuse University, School of Information Studies

skhawaja@syr.edu

Abstract

This paper studies the perception of Users' privacy and its protection with regards to interaction with a hyper-connected information environment, in an effort to show that protecting Users' information in cyber-space from maleficence is a shared responsibility among several stakeholders; regulators (public and private), Information Architecture owners (organizations) and Users. The paper also draws attention to the need of a comprehensive framework for guiding the advancement of future Information Architectures. A framework that involves all stakeholders and serves to protect the Users' data and privacy.

Keywords: User Privacy, Hyper-connected Information Architecture, Smart-devices, Internet Law. Internet-of-Things.

Hyper-Connected Information Architecture and Users' Privacy Protection

Information Architecture has been studied by many names and aliases in one form or the other longer than the documented history goes. Since before humans started to document, they must have started to organize that data and information in some way mentally and for the sole reason for it to serve a purpose at a later point in time. Today, it seems almost unfathomable that there was a time before the advent of the world wide web.

Within the last decade, interest in Information Architecture has garnered incremental focus as more and more products and services are added to the hyper-connected "smart life" that an individual User lives in the internet. Earlier research (Martin, Dmitriev, & Akeroyd, 2009) high-lighted six aspects that were of concern for advancement of Information Architecture. At the top the list was; Information Quality (Searchability, Findability, Accessibility, Security). This is at the core of today's hyper-connected Information Architecture. Searchability, Findability, Accessibility and Security are also the aspects that directly impact the Users of the Information Architecture. This paper will focus on the aspects of an IA that are not only invisible to the User during interaction, but also employing non-browser modes of interaction, for example; through a dashboard, through a smart-device or through an Internet-of-Things device.

An Invisible Information Architecture

The level of personalized services a user can imagine in today's hyper-connected world is only encouraged by the advancement in internet-of-things and smart devices. From something as basic as a user getting his/her physical activity and appointments on the smart-watch, to analyzing patients' bio-signals through a Bluetooth device in near real-time and predicting a cardiac event, days before it happens and alerting the patients' care-provider. From getting notifications about changes to flight departure gate on automobiles' windscreen over-head

display, to having milk and eggs automatically added to the weekly shopping cart because the fridge notified the grocer. These are examples of an invisible Information Architecture. The Users' data which may include private data are exchanged among the inter-connected systems seamlessly without the User ever entering a command in browser or clicking a link.

Individual Privacy has always mattered, or has it?

A longitudinal study about Privacy in the Information Age (Downing, 2016) discussed that Users' concerns about Privacy had not changed over the period of the study, but what was interesting that Users were willing to forego the Privacy, should a steep discount be part of the equation. Without painting everything with a broad brush, it is safe to say that individual Users were willing to share control of Users' Privacy at a price X, whatever that X may be. What is interesting is that Users' are becoming aware about the significance of individual User data in the cyber-space and interested in monetizing it. Which brings us to the fuzzy nature of Privacy when we talk about information architecture, same user interacting with 2 different Information Architectures may have a different state and level of Privacy for each of the IAs.

Multi-state Privacy in cyber-space

In the physical realm, something is either private or it isn't. When the notion of Privacy is discussed with regards to cyber-space, this concept changes in more ways than one. In a hyper-connected information environment, Users' Privacy has multiple states that can change over time and geo-location. Prior research (Bradberry & Nemati, 2014) shows that Users' Privacy is in a constantly transient state, changing from one value to the other. The change of state can directly or indirectly affect its worth. This supports the monetization of Users' Privacy discussed earlier.

Not just Users

Another aspect that has come to light with great discussion on the anonymity that cyber-world affords its Users, is that Users are also people living in the physical world. A recent research (Cornwell, 2013) showed that there are gaps in governance when physical and cyber-world are inter-mingled. These gaps sometimes have serious moral and legal repercussions. Protecting the Users' Privacy should be treated more than just a system compliance check in the enterprise system development cycle. With ever-present hyper-connected information environments and profit-driven open markets, the exploitation of Users' information is something everyone connected to the web worries about.

Gaps in Privacy Protection

Technological advances in the smart-Health arena make them one of the most sought-after with respect to the benefit they promise to the Users. These are also the applications that exchange the most private and critical of data between the User and Information Architecture. Earlier research (Addonizio, 2017) discussed that the current frameworks and models are not enough for safeguarding individual Users' Privacy. We need to extend current regulatory frameworks to include implications in the cyber-world. From the technological perspective, the speed of evolution is leaving a long trail of diverse and inconsistent Information Architectures that are obsolete as soon as they are deployed. The new regulatory framework should be inclusive of technological advances and should stabilize this evolution.

Everyone is trying

Current lack of a comprehensive framework leaves everyone to fend for themselves, be it country blocks like European Union, Country (Cohen, 2012), State (Spann, 2016) or even individual. The same is done in the enterprise sector with organizations fending for themselves.

The issue of Users' Privacy in a hyper-connected Information Architecture is too complex for a single faceted approach, so in addition to the regulatory framework, on the technology side, we need an adaptive framework for measuring compliance of an information architecture. Users are one of the most important stakeholders, so User education and awareness should be part of new framework. User education leads to trust-building which potentially leads to a business transaction, so both public and private sector gains from a more aware and educated User base.

Discussion

Information Architectures employed by the hyper-connected applications, exchange Users' information through complex modes and mechanisms. The added complexity is amplified by having multiple stakeholders and different levels of stake in the information echo-system. With advances in technology and infrastructure, "smart-living" has started to overlap physical-living in many areas of life. Concerns about Users' Privacy Protection are not mitigated well by using the currently available frameworks of governance. Discussion about significance of Users' Privacy is not new and research shows that with time, Users do not become complacent about implications of Data and Privacy in the cyber-world. Research also shows that when it comes to cyber-space, Users' Privacy is not binary in nature. This also opens a world of vulnerabilities and ramifications that come with it. Stakeholders at all levels are increasing efforts in protecting their jurisdiction. Since it concerns individual Users' Privacy Protection, there is a clear need for a comprehensive framework to collate resources for regulation, guidance and education about Users' Privacy and its protection in information environments.

Conclusion

With regards to the hyper-connected Information Architecture of present and future, User is at the center of information ecology which consisted of *Users*, *Content* and *Context* more than

ever before. In today's Information Architecture, User is not only the *User*, but may be the *Content* creator and may also be part of *Context* through location or state. It seems like it revolves around the User, because it is supposed to be invisible. That is when the Information Architecture is at its best. Exchanging personalized relevant information without manually inputting/seeking it and having it available when needed, sometimes even before needing it.

Voluntarily or otherwise, in parallel to the physical realm people beings live in a hyper-connected cyber-reality and continuously exchange information between the two. Data and information flow between the individuals' physical and cyber realms seamlessly with vulnerabilities of all shapes and sizes even when the Users' life depend on it. These vulnerabilities when exploited, can have serious moral, legal and even life-threatening consequences. It is almost impossible, if not irresponsible to leave the obligation of safeguarding the individual Users' Privacy and the pertaining concerns to one single party.

A new type of governance is needed for safeguarding the new overlapped state of Users' information and Privacy. Further research is needed to collate a comprehensive framework for evaluating compliance of all stakeholders at public, private and individual levels in this pursuit of a future information architecture that can be adaptive, progressive, efficient, secure and safe. All without compromising the individual Users' Privacy.

References

Addonizio, G. (2017). The Privacy Risks Surrounding Consumer Health and Fitness Apps, Associated Wearable Devices, and HIPAA's Limitations. *Law School Student Scholarship. Paper 861.* Retrieved from http://scholarship.shu.edu/student_scholarship/861

Bradberry, C., & Nemati, H. (2014). Privacy Momentum: A New Contextually Dynamic Conceptualization of Privacy. *Emerging Issues in Information Security.* Savannah: Twentieth Americas Conference on Information Systems.

Cohen, J. E. (2012). Configuring the Networked Citizen. Retrieved from http://scholarship.law.georgetown.edu/facpub/803

Cornwell, J. K. (2013). Sexting: 21st-Century Statutory Rape. *SMU Law Review, 66*. Retrieved from http://scholar.smu.edu/smulr/vol66/iss1/41

Downing, C. E. (2016). Privacy and The Information Age: A Longitudinal View. *Journal of International Technology and Information Management: Vol. 25: Iss. 2, Article 3.*

Martin, A., Dmitriev, D., & Akeroyd, J. (2009). A Resurgence Of Interest In Information Architecture. *UK Academy for Information Systems Conference Proceedings 2009. Paper 35.* Retrieved from http://aisel.aisnet.org/ukais2009/35

Spann, S. (2016). Wearable Fitness Devices: Personal Health Data Privacy in Washington State. *Seattle University Law Review, 39*, 1411-1432.