Chapter 102
Volunteered Surveillance

Subhi Can Sarıgöllü
Istanbul Bilgi University, Turkey

Erdem Aksakal
Istanbul Bilgi University, Turkey

Mine Galip Koca
Istanbul Bilgi University, Turkey

Ece Akten
Istanbul Bilgi University, Turkey

Yonca Aslanbay
Istanbul Bilgi University, Turkey

ABSTRACT

As the front end of the digitized commercial world, corporations, marketers, and advertisers are under the spotlight for taking advantage of some part of the big data provided by consumers via their digital presence and digital advertising. Now, collectors and users of that data have escalated the level of their asymmetric power with scope and depth of the instant and historical data on consumers. Since consumers have lost the ownership (control) over their own data, their reaction ranges from complete opposition to voluntary submission. This chapter investigates psychological and societal reasons for this variety in consumer behavior and proposes that a contractual solution could promote a beneficial end to all parties through transparency and mutual power.

INTRODUCTION

This chapter explores the human experience and cyber cognition aspects of cyber security from a consumer point of view with macro-micro transitions at various levels. It primarily focuses on some of the root causes and the cognitive dimensions of cyber security and explores the societal and psychological dimensions of cyber security from consumers' point of view. Then it concentrates on online consumer experience over the case of Ad Blocks, elaborating on the asymmetric positioning of the consumer on

DOI: 10.4018/978-1-5225-7113-1.ch102

the reallocation of power, and ownership aspects. The study proposes a potential approach of balancing the asymmetry by an alternate way of shared access to consumer data. Finally, it concludes by introducing further concerns on cyber security and security in general that comes with the transformed version of cyber cognition.

Danger and fear are very primordial and deeply embedded into human existence and reasoning in every context. As relatively interim solutions, social structures, systems and all varieties of mechanisms have been created to overcome the danger and fear along with their long-term repercussions that have been shaping human evolution, cognition, individual and collective behavior since the beginning of history. Armies, states, belief systems, concepts of ownership and possession, legal and financial systems are the solutions reasoned and created for this primordial urge of being safe, and away from danger. In that perspective ownership, privacy, security, and protection have always been services and products that are deeply rooted in the markets of minds which are in constant evolution. The notion of security comes with cognition of our physical being (Lakoff & Johnson, 1999; Heidegger, 1996) and very much linked to the notions of danger, threat, and fear. Heidegger interprets fear and dread as critical modes of disclosure of the being, as a tool to understand, clarify and deepen our understanding of being in time (Heidegger, 1996). While considering the dynamics amongst human psychology, physiology, behavior, cognition, sociology and cyber security, the perceptions of fear, danger, and security play a critical role.

The rapid transformation of living standards across the globe during modern and postmodern eras have shifted perception and thought patterns along with the dynamics and structures that are regulating them (Lakoff & Johnson, 1999; Belk, 1988; Massumi, 1993). Especially the latest developments in the ICT arena- increased access to the internet, mobile device usage, social media usage and the arrival of IoT, shift individual, societal, commercial, administrative, financial, legal, ecological and cognitive landscapes to another dimension (Lakoff & Johnson, 1999; Massumi, 1993; Prensky, 2009). These shifts deepening the crack in the digital divide, the gap between the speed of technological and digital advancements and the speed of social systems and mechanisms to adjust, to protect and to cope with misuse, frictions, crime, escalates the individuals and smaller enterprises to a more vulnerable position. On September 7th., 2017, Equifax, a more than a century old US consumer credit reporting agency, has declared a major data breach affecting more than 143 million US consumers (57% of adults in the USA), 100,000 Canadians and 200,000 UK citizens. Social security numbers, personal ID details, credit card details are amongst the types of data that were breached. The current state of cyberspace can create such major susceptibilities.

Our living/offline world and digital/online experiences and their contents play a very critical role in shaping our perceptions and cognition of reality, danger, safety and security and our capacity to reason (Lakoff, 2009; Varela, Thompson & Rosch, 2017). Developments in cognitive science converging with technological advancements in all fields from genetics to physiology, artificial intelligence to physics take place at such a speed that human cognition has not experienced, processed, and internalized before. The speed of these developments becoming a part of everyday life of individuals, societies, and masses and the speed of societies and individuals to fully comprehend and master these developments are not synchronized. On the contrary, with the emergence of big data, advanced analytics, and the full-grown information society, previous asymmetries among social members and stakeholders have been increasing more than ever. It can be easily presumed that as the speed of development increases, the time, energy, and investment required for adjustment of the growing masses will tend to increase. Clearly, this transformative meta-process from post-modern times to a new era has no patience to stop and wait for all