Privacy Concerns in the Age of Smart Devices

Solomon Negash and Peter Meso

Mobile phones, tablets, wearables, and Internet of Things (IoT) technologies have become ubiquitous. These devices, collectively termed Smart Devices, have shifted the way personal information is collected and used by companies, hence, raising critical information privacy concerns (IPC). A survey found that 9 out of 10 adults believe they've lost control of how their personal information is collected and used. In this paper we discuss some of the trends that have contributed to the shift in personal IPC and recommend key features that should be included when studying individuals' IPC. The academic literature has identified IPC first order constructs; in this paper we identify second order constructs for IPC that have emerged as a results of the Smart Devices era we now live.

Smart devices are always connected to the Internet making them vulnerable to hacking and malware exploits. Personal information of an individual logging through a third-party, like social media, would still be vulnerable. The FTC warns that signals emitted from mobile devices can be used to track individuals and this kind of tracking is invisible. Location-based and cross-device tracking can link different devices and create a digital fingerprint to link consumers to multiple devices. Despite these vulnerabilities, Smart Devices do not have even the level of privacy protection afforded to traditional computers.

TRENDS CONTRIBUTING TO PRIVACY SHIFTS

We identify seven core trends contributing to the shift in IPC including: Active-to-passive shift in data collection; blurring of distinction between personal and corporate assets; asymmetry of power between consumers and corporations; commoditization of data; cloud services, B2B systems integration**,** and IoT integration.

Active-to-passive shift in data collection. In the era of Smart Devices personal data is shared (or shareable) without the knowledge of the consumer. This is because collection of such data has now become passive – performed ubiquitously and surreptitiously by the sensors and other data-collection mechanisms built into these Smart Devices. This trend shows that collection of consumer information has shifted from being actively provided by the consumer to passively accessed without the consumer's knowledge.

Blurring of distinction between personal and corporate data. Trends like Bring Your Own Device (BYOD) have blurred the distinction between personal and corporate assets. The ability of corporations to monitor employee is not new, but in prior eras the employee information was often accessed through a computer provided by the company or through direct online or offline conversation with the employee. In the era where the distinction between personal and corporate assets are blurred the potential for divulging unintended personal information has increased, where employer and employee may find themselves in adversarial positions.

Information power asymmetry between consumers and corporations. Information asymmetry has given corporations more knowledge when bargaining with consumers. The ability to accumulate and manipulate data gives corporations' asymmetry of power.

Commoditization of data. Big data, analytics and artificial intelligence are merging to form analytics commoditization. The personal data needed for purchasing products and services has itself become economical, now the personal data can be traded or monetized. Commoditization of data driven by analytics and artificial intelligence has altered the meaning and value of consumer data, increasing privacy concerns.

Cloud services. With the popularity of cloud services, one of the shifts is that third-party vendors hold most of the sensitive data. This has given cloud services providers unfettered access without privacy contractual agreement with the consumer. Corporations are the primary customers of cloud services providers, not the consumer. The distance between the data custodian (cloud services provider) and "real" owner of the data (consumer) increases the susceptibility for unethical behavior.

B2B Systems Integration. This B2B integration has allowed corporations and their supply chain partners to collaborate within and across the supply chain. The personal data silos that were collected by different corporations are now integrated creating a seamless digital profile on billions of consumers. The integration of B2B systems poses greater privacy risks.

IOT integration.

The emergence of IoT brings a wave of wireless revolution expanding privacy concerns. IoT allows advertisers to target ads based on whether you are home or not. IoT has joined the always-connected paradigm, and this ability to amass even more personal data increases privacy concerns.

SECOND ORDER CHARACTERISTICS FOR IPC

We posit that the trends discussed above have altered the collection and use of consumer data leading to the emergence of second order characteristics that go beyond the first order characteristics identified in prior research. The six first order characteristics from prior research and the proposed second order characteristics are listed in the table below.

First Order Characteristic	Second Order Characteristic
1. Collection	
	1a. Overt Collection
	1b. Concealed Collection
2. Secondary Use	
	2a. Internal secondary Usage
	2b. Commercial Secondary Usage
3. Errors in Data	
	3a. Data Quality Errors

	3b. Correction of Errors
4. Improper Access	
	4a. Post Collection Improper Access
	4b. Device Improper Access
5. Control	
	5a. Data Ownership Control
	5b. Personal Privacy Control
	5c. Digital Identity/Persona Control
6. Awareness	
	6a. Disclosure Awareness
	6b. Informed Consent Awareness
	6c. Unknowable Data Awareness

In summary, the almost universal adoption of the always-connected smart devices means that access to personal information by external entities is much more pervasive, multifaceted, and quite likely perpetual. Further, mechanisms that provide for such access are increasingly surreptitious. This unprecedented access capability thus allows for collection that is equally surreptitious, pervasive, multifaceted and also perpetual.

In our presentation we will include a testable theoretical model and questionnaire items.