BLG PUBLICATION

Borden Ladner Gervais

Internet of Things: OPC Publishes Research Paper on Privacy and Security Risks Associated with Retail and Home Environments

The Office of the Privacy Commissioner of Canada ("OPC") last week published a new research paper on the Internet of Things[1]. The paper focuses, in particular, on issues of privacy and security in retail and home environments.

The Internet of Things is the generic description given to the ability of everyday objects to connect to the internet and/or communicate with other devices or objects. For example, radio-frequency identification (RFID) chips imbedded into goods or objects permits real-time tracking of the objects to which they are attached. Devices and/or objects can also transfer small amounts of data quickly and imperceptibly through near-field communications (NFC) or communicate directly with each other or larger systems.

While interconnected devices and systems are not new, technological advancements such as smartphones and the development of low-cost sensors and wireless networks, have significantly increased the ability to monitor, gather, and communicate information about the devices themselves and their environment. It is possible to gather extensive data about the habits and patterns of individuals based on the uniquely identified mobile devices they carry with them. The amount of data as well as its quality and precision will increase in the future.

The OPC cites forecasts which predict exponential growth: for example, ABI Research predicts that the number of connected devices will increase from 10 billion to 30 billion by 2020, while Cisco Systems forecasts that there will be 50 billion devices connected by that same year.

Internet of Things in the Retail Sector

The prevalence of smartphones and other connected devices in conjunction with the spread of wireless hotspots, Bluetooth, and other networks in public spaces has dramatically increased the amount of information which can be gathered both visibly, such as through smartphone applications associated with loyalty programs, and invisibly, such as data gathered from interactions with a device's radio interfaces (i.e. Bluetooth or WiFi). Retailers can use this data to improve efficiency, through better inventory management and store layouts, or to direct promotions to customers who are in and around their store.

The OPC focused on the issues associated on the invisible collection of information: where small amounts of data including, a device's unique identifier and general location, can be collected without the device connecting to a network. The placement of networks of sensors or beacons in public spaces and retail stores can make it possible to track the movement of electronic devices, and the individuals carrying them, across a large geographical area. These same networks could also be used to send targeted messages or promotions to those devices.

Privacy Concerns

The OPC identified a number of privacy concerns associated with the invisible collection of information about electronic devices. First, even though the data is linked to a uniquely identified device, rather than an individual, the OPC and other entities consider the information collected to be personal information. The reason is that the amount and quality of the data gathered on electronic devices makes it possible to identify individuals and

reveal their habits or preferences when this is combined with other publicly available information.

Another privacy concern identified by the OPC is that individuals are generally unaware that this information is being collected and, as such, are not able to consent to its collection. The OPC was of the view that the existing consent model, which involves a one-size fits all consent, is inadequate and a more nuanced approach is required where consent can be time or location limited. Possible approaches identified by the OPC include creating rules for machine-based decision making or allowing the devices to "learn" what is acceptable behaviour.

A further issue identified by the OPC is that it will be extremely difficult for individuals whose data has been collected to ensure the accuracy of the collected data and to determine which entity to hold accountable.

Security Concerns

The interconnectivity of the devices which make up the Internet of Things will also increase the privacy and security risks faced by organizations and individuals. The large amounts of information that is gathered, or the information gathering devices themselves, will be vulnerable to attack and/or the theft of data. Similarly, the linking of smart appliances, such as remote power outlets, door locks, televisions and webcams as well as security systems that are controlled from smartphones with in-home networks will increase the vulnerability of these networks.

One of the primary sources of risk is that the sensors and simple internet-enabled devices which make up much of the Internet of Things tend to have low security and/or weak encryption capabilities due to "limitations on power, computing capacity, and other factors." This means that firewalls and other security features are unavailable or ineffective. New security solutions or network controls will be required.

Conclusion

The importance and reach of the Internet of Things is expected to increase exponentially in the next few years. As this occurs, privacy and security risks will likely continue to increase. Further research and development will be required to unlock the benefits from the collection of this additional information as well as to mitigate the new privacy and security risks. We may also see governments explore new ways to address consent to the collection, use, and disclosure of information about electronic devices.

[1] The Internet of Things: an Introduction to Privacy Issues with a Focus on the Retail and Home Environments

AUTHOR

Roberto Ghignone
T 613.369.4791
RGhignone@blg.com

Borden Ladner Gervais

BLG OFFICES

Calgary

Centennial Place, East Tower
1900, 520 - 3rd Avenue S.W.
Calgary, Alberta, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, Québec, Canada
H3B 5H4

T 514-954-2555
F 514-879-9015

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, Ontario, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Toronto

Scotia Plaza
40 King Street West
Toronto, Ontario, Canada
M5H 3Y4

T 416.367.6000
F 416.367.6749

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, British Columbia, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415