A Special Feature Brought to You By **Singapore Management University**

Hidden dangers of digital intermediaries

While they are useful, there is also a dark side to the medium, says Robert J. Kauffman

A MAJOR technology-led innovation in the past twenty years has been digital intermediation. Today, Google delivers handy search services, Instagram offers photo sharing, and Facebook lets us keep in touch with friends. Mobile devices and the Internet support location tracking and contextual awareness to improve the customer's shopping experience. Digital intermediaries, meanwhile, offer other useful services too: job search; investment management and securities trading; mobile and peer payments; travel and hospitality price comparisons and bookings; and all kinds of location-aware information to support shopping.

Digital intermediation has created new opportunities for businesses and transformed the consumer experience in the process, in a lot of 'know me better' ways. These days, businesses can count on consumers being better informed than ever before too. Shoppers can gain an understanding of the evolution of prices during the past couple of years for their favourite brands of digital cameras or computers, forcing the manufacturers and retailers to be effective with product line development, pricing and promotions.

It is also easy to get a sense of the quality of services at hotels and resorts in distant places where we plan to go on vacation, through many digital sources. We can even book collaborative home-stays around the world through Airbnb and other intermediaries. And taking advantage of real-time predictions for future airline ticket prices between almost any two points in the world is easy now. The valuable services of digital intermediaries are there to help and guide us.

Information and privacy
But there is also a dark side to digital intermediation in the markets these days. A source of concern for retailers, for example, is the extent to which their payment intermediaries for consumer purchases, especially the credit card companies VISA and Mastercard, now know so much about retail customers' merchant choices, spending categories and purchasing patterns.

The value of such information is extremely high, and tightly held by the card intermediaries. That's a major theme here: the intermediaries know a lot about us, probably more than the merchants and we are becoming increasingly vulnerable because of how much the world knows about our economic and social activities. Digital intermediaries wield an enormous amount of power in the markets where they operate – and this is a sea change from ten years ago. Some travel and hospitality industry observers have noted that the airlines and hotels struggle with the 'ownership' of their customers now. Companies such as Orbitz, Travelocity, Expedia, and others are now the new digital intermediaries in the marketplace; the direct relationships between the original service suppliers with their customers have been disrupted.

The intermediaries now have more complete views of customers' flight and hotel bookings across many different service providers, while the suppliers only have knowledge of their own reservations. This gives the intermediaries the upper hand with creating new perceptions of value for customers; the suppliers have difficulty achieving a compelling brand promise, as a result. Finding ways to encourage customers to make direct-from-the-supplier purchases has become more costly and difficult too. So managers at large companies wonder: How can we achieve intimacy with customers in spite of the digital intermediaries?

Other observers voice concerns over our potential loss of personal privacy in 'The Great Indoors': where we live, and where we spend our leisure time. How will in-building location identification technologies deployed via mobile phones and sensors open up anonymous tracking of people while they are shopping? The issues are related to possible exploitation of private information on their in-store behaviour and purchases – and other secondary issues that may arise.

Relevant info when you need it
Such technologies also make it possible for retailers to offer context-aware promotions to customers – so the right people receive them at the right time in the right place – with incentives designed to engender positive customer responses and an improved shopping experience. After all, when we shop in physical stores, we have the least information available to us for making comparisons, since we are focused on the offerings of just one seller. Some questions remain though: What are consumers willing to pay to protect their privacy? Or will they exchange it for a simple offer? A one-dollar discount? Buy-one-get-one-free? A loyalty card membership for purchase discounts?

In 2013, Apple announced a location-based awareness support initiative centred on its software and communication protocol innovation, iBeacon. This is built into Apple iOS 7, so it is now loaded into iPhones and iPads that are available on the market. iBeacon supports other inexpensive and small sensing and communications devices that can use Bluetooth, just as the iPhone does. iBeacon as physical sensors support one-way, to-the-customer delivery of parking space locations, in-store shopping offers, micro- location-aware promotions, and other location-based information related to retail stores.

However, their emphasis is on data delivery, not data collection from the customer that would be viewed as too invasive. iBeacon's applicability is not limited to retail. For example, some of the tests of its application have been for seat upgrades and personalised ads in sports arenas, parking garage navigation, and public transit arrivals.

The LiveLabs Urban Lifestyle Innovation Platform at Singapore Management University's (SMU) School of Information Systems (SIS) carries out research to explore how organisations can use mobile phone technologies. It has developed software for managing the power of mobile phones, for assessing mobile phone sensing capabilities, and identifying co-located groups of people. LiveLabs also studies how to leverage outdoor and indoor location-based strategies for delivering context-aware shopping promotions, public information, and other useful information.

Dangers with digital intermediation are present in other well-recognised and widely discussed business and technology contexts too. My research centres on financial information systems and technology, so I have been tracking the dangers of digital intermediation in financial services.

One issue of global interest is the decentralised digital currency, 'Bitcoin', which is not managed by central banks or commercial banks. A single bitcoin's price rose to an all-time high of US$1,236.83 in December 2013. A Japanese digital intermediary named Mt.Gox – a 'Bitcoin exchange' – was estimated by The Wall Street Journal to have handled about 70 per cent of global exchanges of bitcoins in 2013.

Earlier, it had trouble with a hacker, and that led to a crash in the price of a bitcoin in 2011 though. Later, lost bitcoins in Mt.Gox's accounts led to a loss of trust. Then Mt.Gox declared bankruptcy in February 2014, amid allegations of the theft of bitcoins. Some said this was due to the lack of failsafe information security.

This is a poignant example in which the dangers of a single digital intermediary stand out. Mt.Gox damaged trust in the global Bitcoin ecosystem, which consists of 70+ exchanges and software platforms. They support 12.85 million bitcoins in circulation, with a value of US$8 billion as of June 4, 2014. The problem is similar to what can happen when a systemically important international bank has financial problems, creating ripple effects and damage through the global economy.

Mitigating the dangers
At SMU, our research projects are intended to help business and government leaders in Singapore and elsewhere to understand and address the dangers of digital intermediaries. For example, information security research is a special competency at SIS that touches on the potential problems with such firms. In October 2013, research by SMU and the Institute for Infocomm Research (I²R) at Singapore's Agency for Science, Technology and Research (A*STAR) led to the discovery of vulnerabilities in Apple's iOS 7-based mobile phones. Repairing these vulnerabilities probably spared an untold number of digital intermediation services users many problems.

SMU's faculty conduct related research on these issues in the Living Analytics Research Centre (LARC, a joint effort with Carnegie Mellon University). They focus on data analytics for business, consumer and social insights, yet also emphasise proper safeguards for individual information privacy protection and data management. And I do this in my teaching on technology-led social and industrial change; financial, hospitality and transportation services; data analytics; and ethics for applied research on technology.

> 'At SMU, our research projects are intended to help business and government leaders in Singapore and elsewhere to understand and address the dangers of digital intermediaries.'
>
> – Robert J. Kauffman, Professor of Information Systems and Associate Dean (Research) at SMU School of Information Systems

This is a monthly thought leadership series brought to you by the Singapore Management University. Next month's feature will discuss how SMU develops Asian business insights and shapes the practice of management.