

Exploitative, Unethical, Criminal? The Use of Technology in Commercial Marketing

PROFESSOR MARK GRIFFITHS*

Technology continues to invade almost every area of our lives. Although the advantages of these technologies outweigh the disadvantages, technology is increasingly being used in commercial settings that some citizen's rights groups claim are exploitative, unethical, and border on the criminal. This article briefly outlines some of these perfectly legal practices all of which raise ethical questions about the invasion of people's rights.

Shopping loyalty cards are now an every day part of consumer behaviour. Most people probably don't stop to think about the reasons behind their introduction but they have the potential to be exploitative. In short, loyalty cards track every purchase a consumer makes over a three-year period including the store shopped at, the date and time, and the price paid. The three-year period allows for monitoring of trends in purchasing. Stores may also record the method of payment, whether the card was swiped or keyed into the till, and the checkout that was used. The supermarkets use these data to categorize customers. In addition to the data provided when the loyalty card was issued, commercial operators can draw conclusions from the address using sophisticated categorization systems. Many companies now use customer relationship marketing software to help make sense and synthesize the information gathered. Ever since they were introduced, underhand uses of loyalty cards have been mooted. As long ago as 1999, the Ministry of Agriculture suggested cross-checking purchases of genetically modified food with health records, effectively making the cards part of a huge medical experiment. However, the supermarkets declined to take part.

It's probably a fair assumption to make that the online population sees the Internet more as a tool for information gathering and communication than for commercial transactions. The most powerful impacts are social rather than commercial. Just like the companies who run loyalty card schemes, Internet service providers can record when you logged on and off, how many seconds the connection lasted, and the Internet protocol address allocated during the session. They can also compile a detailed e-mail history. This can contain the header information from every e-mail received by the account in the period, the return address provided by the sender, the ISP from which the e-mail originated, the date and the time of the sending, an ID code, and the title of the e-mail. Most people have no idea how much potential there is for invasion of privacy.

There are some areas that are potentially more worrying than others. Take the case of online gambling. When it comes to gambling, there is a very fine line between

providing what the customer wants and exploitation. The gaming industry now sells gambling in much the same way that any other business sells things. On joining Internet gambling sites, players supply lots of information including name, address, telephone number, date of birth, and gender. Internet gambling operators will know the player's favourite game and the amounts they have wagered. Basically they can track the playing patterns of any gambler. They will know more about the gambler's playing behaviour than the gamblers themselves. They will be able to send the gambler offers and redemption vouchers, complimentary accounts, etc. Supposedly all of these things are introduced to enhance customer experience. Benefits and rewards to the customer include cash, food and beverages, entertainment and general retail. However, more unscrupulous operators will be able to entice high spending problem gamblers back onto their sites with tailored freebies (such as the inducement of "free" bets).

The Internet also appears to be a rapidly growing medium for child-oriented marketing with sites ranging from *pokemon.com* and *barbie.com*, to *lego.com*. These sites provide what appears to be a safe environment for children to play in online. Today's children are computer literate and the Internet empowers them to influence what they want for Christmas or their birthday. However, how ethical is it for businesses to use advertising to pitch to children – individuals who in most other spheres (eg, voting, sex, legal documents) are treated as incapable of making decisions. Many claim the adverts carry a similar message (ie, "If you haven't got this product, you are abnormal"). The aim of most marketing is to sell goods, but adverts aimed at children are designed to get them to pressurize their peers and parents.

The US Center for Media Education (CME) claim that advertisers and marketers exploit children by advertising products on the Internet in ways that manipulate children and violate their privacy. They have urged the US Federal Trade Commission to develop safeguards for children and claim that these advertisements would infringe American regulations that put safeguards on broadcast media like the television. They recommend that there should be no children's content directly linked to advertising and that direct interaction between children and product spokescharacters (such as *Kelloggs* "Tony the Tiger") should not be allowed.

The CME claimed advertisers use a variety of online methods (like "infomercials") to collect detailed data and compile individual child profiles. This information is then used to establish direct and intimate relationships with children online. The CME claim children's privacy

* Psychology Division, Nottingham Trent University.

is routinely threatened to encourage children to disclose personal information about themselves and their families with some sites offering gifts and prizes. This technology makes it possible to monitor every interaction between the child and the advertisement allowing firms to create personalized marketing for a child. Again, questions need to be asked about how far advertisers can go and what protection vulnerable groups should have.

Other new technologies are also making an impact – often without the person’s knowledge. For instance, television set top boxes can monitor viewer activities. Those who operate set top boxes say they are doing it in order to develop personalized advertising. However, many claim that Internet video providers should not be able to track and sell information about what you viewers are watching in the privacy of your own home. Companies who use these systems claim they only keep anonymous viewing information. They also stress that their viewers can opt out of the data collection but the reality is that very few do. Perhaps the best way forward is to see the introduction of “opt-in” rather than opt-out clauses.

The next generation of set-top boxes are being designed to record the viewing and spending habits of the viewer. Profiles can then be formulated from databases using a range of data including age, discretionary income, parental status, psychographic data, and demographic data. This data can be analysed and made available to marketers, advertisers, and programme makers. In a nutshell, the interactive TV industry is making wholesale use of “personally identifiable information” (ie, names, addresses credit card numbers, etc). Despite the fact that it’s still relatively early days for this type of technology, the use of such invasive technologies does raise fundamental questions about people’s every day rights.

Given the increasingly sophisticated technology on offer, companies have to do a lot of planning to get most out of their databases. There are two main sorts of database.

The first type is a “flat file” databases with information on them, set one after the other. The second type is a “relational database” that can build relationships between different fields of information. For instance, if a company wanted to find a number of customers who had bought a particular product from them in the last month or sort their customers by their address, a flat file database could do those tasks individually whereas relational databases would do it simultaneously. The really creative part (and some might say potentially exploitative and unethical part) in database use, starts when companies begin to look seriously at what the information can do for them. This is the stage when companies start to ask intelligent questions about the actual purpose of the information they have gathered.

Over the last decade, customer relationship management (CRM) has become integrated with database management. Companies offer insight into CRM processes that become available when information is managed electronically. Analytical CRM is geared towards understanding a series of interactions with customers over time in activity-based terms, with a view to understanding whether a given customer is profitable to the company and satisfied with the quality of that relationship. For this to work, the company needs in-depth detail on finance, human resources, distribution, and manufacturing so that they know exactly what a customer is costing them. Companies then know whether the customer is worth hanging on to. While the majority of companies may be using CRM for genuine customer enhancement, there are always those who are less scrupulous and may use such information to exploit.

Even a brief examination of how technology is being used in commercial situations demonstrates that the potential for exploitation of the customer is ever present and that such technologies should be monitored closely. Whether any of these practices will be seen as in some way criminal in the future remains to be seen.