Mark Chipperfield

is a Chartered Marketer, FCIM,
FIDM, DMA Data Council,
IDM Data Council, and Head of
Data Management at BBC TV
Licensing.

Opinion Piece

Consumer concerns: The opportunity for direct marketing? or How a shared responsibility on consent and data maintenance, the environment, and data security could provide the renaissance for direct communications

Mark Chipperfield

Received: 14 August 2007

Keywords: direct marketing,
data ownership, social responsibility,
consumers, security

Abstract

This opinion piece explores the relationship between consumers, their data and the Direct Marketing Industry. The author looks at how the balance of data ownership and management may shift toward the consumer in the battle for trust, and in relation to both environmental responsibility and fending off of further industry legislation.

Journal of Direct, Data and Digital Marketing Practice (2007) **9**, 117–121.
doi:10.1057/palgrave.dddmp.4350087

Introduction

Companies that use Direct Marketing and Data users need to think carefully about the relationship they have with data, where it comes from, how they get it, how they use it. They need to think more about the Consumer perspective generally, but also about Security and about Social Responsibility. In this brief opinion piece, I want to explore the following areas.

- Are we seeing changes in the Value Exchange that occurs between the corporate data owner (client company or commercial data owner) and the end customer, that providing personal data is part of? Is there a new Tipping Point between Privacy and concern over Security and the Desire for great Customer Experience?
- What are consumers prepared to trade for better service, better price or value or the opportunity to save time, in order to be part of

Mark Chipperfield
Head of Data Management
BBC TV Licensing
MC5 A3 Media Centre,
Media Village,
201 Wood Lane,
London, W12 7TQ, UK
Tel: +44 020 8008 2461
E-mail: Mark.Chipperfield@bbc.
co.uk

- a particular community or customer set? And should they even expect financial reward for providing information about themselves — lifestyle companies and suppression companies paying in to their personal accounts for data used? — I like this idea personally!
- Can they have it all? Can a consumer demand control over their data and have these things or will the separation between data owners or the businesses providing their services and products and the end customer continue much as it does now?

Data paradoxes

There is an undisputable trend in what could be termed ‘data usage awareness’ and willingness to act among consumers. This is demonstrated in the exponential take-up of the TPS in recent years, growing volumes of data-related complaints to the ICO and other agencies and direct to companies, such as complaints about misapplied preferences and incorrect details, together with continued media scaremongering. At least in part this reflects a reality of genuine concern about information proliferation and abuse — spam, smart card tracking, video surveillance, ID theft and so on. This trend nevertheless stands alongside a growing expectation for ‘joined up information’ that is to say, people expect data to be collected and then used intelligently when communicating (or in not communicating) with them. Whether or not this paradox can be squared or explained, it is real, like the demand for cheaper *and* better or more *and* greener. Younger generations expect to provide information in the new electronic channels and for it to be protected, but also relevantly and actively used in communication with them. Like the generation before them, they hand out data about themselves to ‘carefully selected’ companies, trusted service providers and, probably, on occasion, some companies that they are not actively doing business with just yet, if ever.

Another related apparent paradox is also worth noting, specifically with respect to financial data and credit. In this case there is, on the one hand, heightened concern about account takeovers, phishing, identify and general data thefts, while on the other there is a growing disassociation from personal blame (it’s someone else’s fault) when things go wrong. While the individual hears stories about data theft, and takes certain additional steps to secure their data, there is also an apparent perception that we are not largely responsible if some criminal element does misuse our data. This is of course compounded, and to a degree made sense of, by the financial industry and its business merchant customers’ willingness to swallow losses from fraudulent activity and misuse of identity.

Data management and government

In today’s world, there is a genuine and often practical difficulty in withholding information or guarding it or keeping track of all our data, even if we wanted to. The government is periodically and perhaps rightly considering data sharing across and between departments. This is both to provide better customer experience to the citizen — so that they do not have to deal separately with multiple government departments when their address or circumstances change and provide administrative efficiencies. But also potentially to identify gaps or even

‘contradictions’ provided within the data — some might say this is the first phase of Identify Cards by stealth — but certainly to support the criminal services in identifying possible criminal activity. Both best practice and data protection law for commercial and non-commercial organisations demand that we only capture data appropriate for the specific ‘relationship’ or purpose, and that we store and maintain it — *use it*.¹ When individuals apply for things, they will often have to provide several and various forms of ID to companies, who are neither Government nor agencies of Government, but who also demand security or the impression of providing security at least. In other words, information is passing through our hands constantly. We may try to be careful, but we are also partaking in a growing number of relationships where the exchange of information is necessary, required, part of the value exchange. We are communicated to and with, more than ever before, and that does not just include ‘direct’ communications of course.

The Robertson case where, back in 2001, Mr Brian Robertson, a retired accountant from Pontefract, succeeded in requiring his authority, and ultimately all authorities, to implement an opt-out mechanism on the electoral roll registration forms, seems from somewhat of a different era — in that generally, we are providing more and more data to more and more organisations. It also seems like a sledgehammer approach to crack a nut. Or does it? Supposedly that case, that resulted in the law amendment,² was about the issue of data captured for one purpose being misappropriated and used for other (commercial) purposes. Also that registering on the electoral roll in order to vote was a legal requirement, but which resulted in that data being used for other unrelated purposes without a mechanism to abstain from that. The TPS upturn is similar in that while the law has not been changed, BTplc managed to successfully promote this preference service as a component of one of their own services, and through the power of television advertising ‘tune in’ to the very real concerns around our telephones being called by people we have not personally handed our telephone numbers to. The dramatic increase in the numbers of registrations is well documented in this case, but, like the Robertson case, does it suggest that we would all opt out of all our information being used by companies we do not know, have never spoken to directly or recently, the government or anyone else, given half a chance?

Security and the environment

There is no doubt that individuals are worried about data abuse. Companies are worried about data misuse and what that may mean for their brands and general reputations. Hence, awareness around data security and the very real personal and commercial impacts that data mishandling can result in is evident. As is the growing willingness and awareness of the individual either in their consumer or business personas to highlight breaches of their own data usage. But another issue that is resonating and finding traction with individuals is the Environment, and there’s a connection between these two that could lead to a real shift in how responsibilities are shared when it comes to

data management, and direct marketing needs to take note and take the initiative if it is to retain self-regulation of any shape, and if it is ever to achieve conscious popularity.

The connection starts at the point where simply saying ‘yes’ or ‘no’ to communications and possibly getting to choose channel preferences — for example ‘please mail me but don’t call me’ or ‘e-mail and sms me please but don’t mail me’ and so on — is giving way to the need and, for some, the demand to take ever more control over our own data and how it is used. This for reasons of security in part as previously noted, but also because ‘we can’ and we are getting used to that in order to improve service, personalise content, earn and redeem voucher discounts, change and switch off channels and so on. For the early adopters and the new generations of electronic communicators, the demand to be in control or at least have a say in what they receive, when and by what channel is already well underway. There are segments of the population who have never even received a direct mail letter through the post! Those who simply switched off the telephone channel via TPS to resolve an annoyance issue and those who opted out of the Electoral Roll are only partly and somewhat crudely engaged with this shift. But, could the increasing understanding of our own personal responsibility (as well as businesses’ responsibility) toward the environment — energy efficiency, conservation and responsible resource usage and the surrounding growing legislation on waste management, together with growing awareness around *personal contributions* — carbon footprint, have a direct and substantive impact on Direct Communications and Direct Marketing as we know it? And could marketers start to engage with customers to pre-empt and prepare for this change, a far greater change than opt out within the electoral roll or registrations on the TPS list could have? I believe they really could and must, and that at the same time direct marketing could move away from its ‘claim’ to be capable of being really targeted, and itself make a seismic demonstrable shift in what it really delivers, through more equitable and transparent engagement.

The opportunity for data and direct marketing

While Above the Line media and channels will no doubt face their own carbon challenge, regulation change and general targets in the environmental space — and anyway ‘what line’ some might say, the finger of ‘opportunity’ is firmly pointing at Direct Marketing, with its particular components of ‘personal data’ and personalised physical media in some cases, which makes that perhaps not so surprising. It is an opportunity to lead by example and set that example for other media and channel neighbours that DM integrates with, to also build on. Many commentators have made the point that it is odd that Direct Marketing should traditionally make the claim of being targeted, and at the same time celebrate 2 per cent response rates. Direct marketers know that econometrically, direct marketing has a far greater impact than purely campaign-by-campaign sales results. Nevertheless, the pressure is on to encourage and incentivise consumers and commercial users of the direct marketing channels alike, to manage and maintain their own details, and to, where appropriate, stop communications

where there is no further interest, or reduce the frequency, or opt for changes in delivery channels. Such actions and mechanical data hygiene enablers are also 'results', and positive ones at that, that will provide the industry and users of the industry services with a clear demonstration of joined-up responsibility. At the same time, they can help in joining up information more efficiently and effectively across and within media channels that will really provide improved customer experience and an industry future, and hopefully a self-regulated one at that.

The multiple and apparent conflicting objectives of privacy and security, commercial freedom, customer choice and environmental responsibility can and will need to be worked on and made sense of together. For data owners and service suppliers, there is opportunity, and responsibility. For client companies and their agencies, they must take responsibility for helping customers and prospective customers manage their own data as far as possible, and use self-regulation and positive responsibility to reduce the potential for further legislation. For the consumer, there is opportunity on all fronts. They could conceivably be financially rewarded for supplying and maintaining their data in the future, turning the current model for free provision of data and being detached recipients of marketing material on its head. In addition to managing our carbon impacts, this could be the start of a renaissance of the Direct Marketing industry.

Notes

1. Data Protection Act 1998. Principle 2 'Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes'. Principle 3 'Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed'. Principle 5 'Personal data shall be accurate and, where necessary, kept up to date'.
2. The ruling in the Robertson case came in November 2001 where both Data Protection and Human Rights law was deemed to have been breached and requiring local authorities to allow citizens to object and stop the disclosure of their electoral information to commercial companies. It likely accelerated electoral roll reform and design, which came in to effect in 2002, prohibiting commercial use of the full electoral roll. A subsequent attempt in 2003 by Brian Robertson to prevent the full electoral roll being available to credit referencing agencies, failed.