Chapter 4
How to Monetize Data:
Rules of the Road and Ethical Dilemmas

Lokke Moerel
Tilburg University, The Netherlands

ABSTRACT

This chapter is a continuation of the preceding chapter, where the author discussed the obstacles encountered by established companies when wishing to transform their business models and provides suggestions for improvement of their corporate governance to better navigate the digital transformation. In this chapter, the author provides practical rules of the road for how established companies can monetize their data including some pitfalls for established companies and discusses a number of ethical dilemmas that companies have encountered in practice when implementing new digital technologies and services.

PROVIDE ADDED VALUE WITH DIGITAL SERVICES AND CUSTOMERS WILL PROVIDE MORE DATA

Despite all obstacles, established companies certainly do not have an impossible starting position compared to the newcomers. They usually have large numbers of established customer relationships with associated customer data and often enjoy the trust of their customers. Training algorithms requires a great deal of high-quality data, something that established companies have a head start on. With the Cambridge Analytica data analysis scandal, many people are now aware that the price tag of new digital business models and personalised offers is usually their privacy. Here are opportunities for established companies. You can use data in a fair way. This requires a different mindset, whereby the higher expectations of consumers vis-à-vis

DOI: 10.4018/978-1-7998-4861-5.ch004

established companies are not perceived as an (unjustified) double standard (see section 'Uneven Playing Field Or Lack Of Sympathy?' in the preceding chapter "The impact of IR4 on corporate governance of listed companies"), but are embraced as a positive. High expectations mean a high level of confidence, which is a positive distinguishing factor in the competition with newcomers (Accenture, 2017).[1]

The most important thing is that customers feel that their data are being used to make the services better *for them*, and not just for companies to earn extra income from them through personalised advertising. Trust, good security and privacy are strong assets online. Research shows that people are willing to share data when personalised *value-added* services are provided in return (Accenture, 2019, p. 32). In contrast, lack of data security and privacy are the main causes of loss of trust (Accenture, 2019, p. 36).

A study by the Dutch Consumers' Association (Consumentenbond, 2019) shows that consumers are relatively satisfied with their banks, although there are major differences, and the *big three* (Rabobank, ABNAMRO and ING) score the lowest. The main reason for this is the ratio of costs and the fact that customers of these banks feel that the *bank's self-interest and making a profit are paramount*. This outcome is really the worst possible combination of the old and new worlds and therefore is a recipe for disruption. Rather than capitalising on their existing relationships and their trust, their online services actually undermine their potential competitive advantage. The Dutch online bank Knab stands out in a positive way. It is no coincidence that this online bank was set up outside the established company (Aegon) with a *user-centric* business model. Knab, for example, gives a notification if a better deal is available for its customers (for example, higher interest rates for savings accounts, a better mortgage rate or insurance premium), even if that other product does not belong to Knab itself.

In any event, established companies will have to follow this route. The consent requirements have been tightened under GDPR. Permission must be *given freely*, which means that, for example, access to an online service may not be made dependent on giving permission for profiling for commercial purposes (for example, by including this in the website conditions or privacy policy) (Art. 7(4) GDPR). If permission must really be freely given, then you must make it very attractive for the consumer to give permission. In other words, you will have to offer an *added-value service* that consumers want so much that they give you permission to collect and process their data for it. Large tech companies are constantly inventing new services with the central aim of generating even more data and thus being able to profile customers. This used to be mainly online, but now these companies are focusing on services and *connected products* in the *offline* world to generate data, such as our cars (*connected* and soon *autonomous cars*), our living environments (*smart homes*) and our bodies (*wearables* and *implantables*).

The Trust Paradox – How Can You Get to Know Your Customer Without Losing Their Trust?

Yesterday, Trustworthyness was good enough. Today, only trustability will do. (Peppers & Rogers, 2012)

One of the most important differences between the old and new worlds is increased transparency (Gillin, 2007, p. 14). Where, in the past, a salesman in a physical store could get away with charging different prices to customers (for example, less of a discount for customers entering the store in their business suit), this is quickly discovered online, and *differential pricing* often leads to online outcries (for example, when it becomes clear that airline fares are differentiated based on a customer's type of laptop and search history (e.g. a higher fare if the customer logs on with an expensive laptop directly to the airline site rather than through a discount site). Complaints about this quickly go viral, especially if they are recognisable or are humorous (Peppers & Rogers, 2012, pp. 96-98). The consequence of this increased transparency is that our collective tolerance for unreliable behaviour has decreased online. (Peppers & Rogers, 2012, p. 6 & 24).

Knowing that a customer's interest is not being well served and doing nothing about it is untrustable. Not knowing is incompetent. (Peppers & Rogers, 2012)

In short, it is more difficult to gain customer confidence online. Because customers often have no personal contact, every online indication of *self-interest* is quickly labeled as unreliable. (Zuboff, 2019) describes this strategy in detail and has coined it *surveillance capitalism*. You will therefore have to show active and visible reliable behaviour. You win online trust *by actively watching out for [your] customers' interests, taking action when necessary to protect those interests* (Peppers & Rogers, 2012, p. 21). This requires proactive steps to ensure that customers do not make mistakes in their online order or overlook a service or benefit, e.g. a telecom subscription that would better fit their calling pattern (Peppers & Rogers, 2012, p. 6 & 24). For *knowing* your customer you need to analyse your customer data, to know when a subscription is up for renewal, what type of subscriptions a customer has (mobile, fixed) and the customer's data use patterns, in order to match the best subscription package. But the more customer data a company processes, the more the customers feel they're being watched, which may have a negative impact on trust. So the question is: how do you get to know your customers, without losing their trust? Knab does this smartly by giving existing customers a signal if they miss out on a benefit (even if this means switching to a third-party mortgage).

The Pitfall for Established Parties: ING BANK

In the introduction, I indicated that a strategy of copying elements from the models of newcomers usually has an adverse effect. A striking example is the storm of protests (including from the Dutch Financial Supervisory Auhtority and the Dutch Data Protection Authority) that arose when, in 2014, ING announced its intention to analyse payment data of its customers for purposes of personalised offers from third parties (Wokke, 2014). The processing in question was privacy compliant (ING requested prior consent from its customers), but encountered considerable social resistance. Under pressure from the supervisory authorities and public opinion, ING stopped the pilot program. In May 2019, there was again controversy when ING announced it would start analysing online payment data for personalised offers, this time for its own products and services only. This time, ING offered its customers an *opt-out* option, which has raised complaints that this is not privacy compliant (Autoriteit Persoonsgegevens, 2019). But even if offering an opt-out option would be privacy compliant, my prediction is that social resistance will continue.

The social resistance can in both cases be explained in light of previously discussed principles. Consumers are very aware of the *trade offs* that newcomers offer. The trade off provided by newcomers is free *user-centric,* data-driven services (benefit), with an *indirect* earnings model of personalised advertisements (privacy invasive). The new services make it worth giving up privacy and having to accept the *nuisance value* of personalised advertisements. Established providers like ING, in this example, try to have their cake and eat it too: they offer *paid* services (the costs of which are constantly increasing), and they also carry out personalied advertisements (impacting privacy), the revenues of which the bank exclusively benefits. The misconception of established parties seems to be that personalised offers provide a value-added service for the user, but this is not how the average consumer experiences online advertising. This perspective only changes if the relevant offers are mostly for products that consumers already buy and for which they then get a discount (such as Knab giving a signal if a service already purchased can be obtained cheaper). In marketing jargon, these are called *thank you* offers. The examples that ING gave with its announcement showed that they mainly intended to make offers for other products (in marketing jargon: *up-sell offers*). The above can also be explained from an ethics standpoint. One of the most important rules of ethics is the *human centric* principle, whereby people should not be used as a means to an end (as an instrument), but should always be considered an end in themselves. If personal data are considered to be extensions of the individual (after all, it is a human right), then the exploitation thereof for the sole benefit of the company is the use of peoples' data as a means to the company's own purpose. Offering an opt-out option (and certainly if it is purposely made difficult to exercise, as in the case of ING) does not

help to remove societal resistance, even if it were legally compliant. With a history of lack of customer trust in the banking sector, this action will be seen as a sign of *self-interest*, and trust will erode further.

The pitfall for existing companies is that they often sit on a mountain of data that are a by-product of their existing services (for example, the payment data of the banks are a by-product of their bank account service). The solution for established companies is to stop thinking that they sit on a gold mine of data that is waiting to be monetised. These are precisely the data that the consumer believes were obtained in the context of a paid service and should therefore not be additionally profited from (as the bank already received a fair compensation). Privacy rules also create a barrier, because data that have been collected in the context of the exercise of an agreement may not be processed for other commercial purposes. In this case, data protection regulation requires that an opt-in must be obtained for profiling for purposes of sending personalised offers. To avoid this, the question that established companies must ask themselves is: which new digital added-value services can we offer, which require data analytics and which will the consumer want so much that they will give us permission to collect and analyse their data.

The Control Paradox – Give Users More Control and You Will Receive More Data

Research shows that if you provide individuals with more control over their information (i.e. increasing their privacy protection), they actually end up providing you with more personal information (decreasing their data protection) (Moerel, 2014, p. 46) (Brandimarte, Acquisti, & Loewenstein, 2014). This is called the *control paradox*. For example, if you provide individuals with access to their profile (i.e. 53, married, likes to hike, two children, etc.) through a *privacy dashboard*, individuals do not delete their profile (because it can still be done tomorrow), but actually correct and supplement this information (I have three children, and I also play tennis!). Another example is that if individuals feel that they have control over their data (just imagine a company actually getting proper data protection compliance in place), they are inclined to entrust more data to such company, which *de facto* leads to less protection. A similar paradox is known in other fields. An example here is the introduction of safety belt legislation. This did not lead to the expected reduction in fatalities, as people felt more secure with their safety belt and drove less carefully (Moerel, 2014, p. 47) (Janssen, 1994).

We see that this paradox is applied by GAFA, for example where Facebook now offers users the option to delete their entire account in one go and where all GAFA users are now offered a *privacy dashboard*. This gives people a sense of control, as a result of which they do not choose to erase their profiles. In any case,

it may be clear that new digital players have set completely different communication expectations, as a result of which users expect active *choice* and *self-service* options in their personal digital environment.

The Pitfall for Established Companies

Here too copying elements from the models of newcomers usually proves counterproductive. Where established companies are going to digitise their processes from an *efficiency* perspective, they often start offering customers self-service options. It saves a lot of time and cost if your customers do things themselves! However, if self-service options are not accompanied by innovations in *user experience* (UX), the move to self-service is perceived by customers as a sign of pursuing *self-interest* by the company (which it is). This is nicely illustrated by the survey of the Dutch Consumers' Association cited above, where lack of confidence in the three major banks is explained by customers as: *prices keep going up while we have to do more and more ourselves!* Here, customers see self-service as a means to cost savings rather than experiencing self-service as a value-added service (Consumentenbond, 2019). As long as digitisation by established companies is seen primarily as an efficiency measure rather than a better UX, it will be difficult to convince their customers that they are keeping up with new times, and all initiatives will be viewed with distrust. It is up to the companies themselves to bring about a change in thinking because only then will their initiatives be viewed by customers as authentic.

EXAMPLES: ETHICAL DILEMMAS

Dilemma 1. The risk department of a financial institution develops an algorithm to predict the likelihood of non-compliance with payment obligations of its customers. Divorce appears to be a large predictive indicator for non-compliance with payment obligations under loans and mortgages. The algorithm can predict the chances of a client getting a divorce based on data on social media. Will you include these data as a factor in decision-making?

Reflection. The privacy rules require transparency about what data you collect and analyse and for which purposes you do so. The transparency requirements are often a reason not include this factor in decision-making, as it is likely to be met with resistance from customers (the result of the analysis will be that the company is more likely to sooner realise that a relationship is going to end than the customer itself). Although the United States does not have direct rules for this, companies in practice apply the *smell test*: what would it feel like if this would appear in the newspaper tomorrow? Do I have a convincing story to explain, or do I really look

bad? If the latter is the case, then secrecy is not an option. Sometimes it is an option to be open with customers, for instance by indicating that you can conduct a risk analysis for payment problems in which all kinds of factors play a role and that, with higher scores, the customer can be given a signal and assistance can be obtained to put things in order.

Dilemma 2. A financial institution has developed an authentication tool that – on the basis of analysis of online behavioural characteristics (interaction patterns with devices, preferences for test use, hand-eye coordination, hand-vibration, pressure exerted on tests) – creates a detailed behavioural profile of account holders, based on which an account holder can be recognised if he logs in to his or her online bank account. If the person logging in shows deviant behavioural characteristics, a further identity check is first carried out (to prevent fraud). The algorithm also appears to be able to predict changes in emotional state of mind (increase or decrease in agitation, concentration, uncertainty) and can therefore be used to monitor risk indicators in the state of mind of flash traders (Levin, 2017). The department's best flash trader shows a sharp rise in risk indicators, but his trading patterns are the same. Do you also use this tool for monitoring? Do you intervene based on the results?

Reflection. Monitoring behavioural characteristics for fraud detection is in the interest of the relevant account holder and can be done in a fully automatic manner. Only if a fraud report comes in (someone logs in to an online banking app that does not have the characteristics of the legitimate account holder) is further investigation needed. This investigation then concerns the fraudster and not the account holder involved. This form of online behaviour monitoring is contained and will not have a relevant negative impact on the account holder concerned. The use of the tool for monitoring the behaviour of flash traders involves the continuous monitoring of an employee in his or her daily activities, whereby action can be taken by a direct supervisor. Research shows that employees who are under constant monitoring experience less autonomy and therefore less job satisfaction (Chrirkov, Ryan, & Sheldon, 2011, p. 228). Instead of having the supervisor carry out monitoring, the tool could also be used to give feedback to the flash trader if the risk factors so dictate. With extreme scores, a ping could be sent to HR or a coach to assess whether there is reason for the flash trader to take a break temporarily. This would be in the interest of the employee himself or herself.

Dilemma 3. There is a shortage of a critical prescription drug from a major pharmaceutical company. There are many complaints due to shortages, but in some places, there are excess supplies of the drug. An algorithm is developed to predict demand and to optimise distribution. The algorithm works well; fewer products remain and the number of complaints is drastically reduced. Management is full of praise for better distribution and also an increase in drugs turnover. After a month,

a data scientist discovers that the algorithm avoids distributing the drugs to certain zip codes. What do you do as a data scientist?

Reflection. There must first be an investigation into the cause of the avoidance of certain zip codes. The investigation shows that the zip codes all concern underprivileged neighborhoods. The reason for this is that medication loyalty in these neighborhoods is lower than in better-off neighborhoods. As a result, critical medicines are sometimes not collected from pharmacies. Investigations further show that the explanation for the decrease in complaints is that patients in underprivileged neighborhoods are less likely to complain (*we are not listened to anyway*). The consequence of the redistribution steered by the algorithm is it can lead to newspaper headlines: *pharmaceutical company gives critical drugs to the rich at the expense of the poor.* What is striking here is that the data with which the algorithm is trained does not seem sensitive at first sight (these are not personal data, but hard distribution data from the pharmacies), while applying the algorithm can nevertheless lead to discriminatory outcomes. Another observation is that algorithms often provide insight into certain factors, which, once you know them as a company, can thereafter not be ignored. If it becomes clear that medication loyalty for critical medicines is lower in certain population groups, what societal role does the company have? Should it collaborate with the pharmacies in the neighborhoods concerned to increase medication loyalty in this patient group or redistribute the medicines in order to get the most from the available stock?

Dilemma 4. An algorithm shows that women who are pregnant are substantially more sensitive to life insurance offers. As soon as the pregnancy is over, this sensitivity is gone. As a marketer, are you going to target pregnant women with personalised offers for life insurance?

Reflection. There are different kinds of predictions (Moerel, 2014, p. 11) (Kerr & Earle, 2013, pp. 48-49). *Preferential predictions* predict preferences. *Preemptive predictions* are predictions that are intentionally used to diminish a person's range of future options. Examples include exclusion from insurance or rejecting a loan. This form of forecasting generally has more implications for the position of an individual than when someone receives a commercial offer based on previous preferences. In the latter case, the individual then has the option of whether or not to accept. The dividing line between preferential predictions and preemptive predictions is sometimes difficult to draw, especially when predictions are used for marketing, especially in cases of so-called *influential marketing* or *persuasion profiling*. Although, strictly speaking, these forms of marketing do not take away options from individuals, individuals are influenced in their choices to such an extent (for example, because of their inherent sensitivity to bargains) that it is difficult to speak of preferences and making choices. This form of prediction does not take the perspective of the individual (does he/she actually want this offer?), but takes the

perspective of the company making the offer. The latter uses the personality traits of the individual (e.g. sensitivity to bargains) and often not previous preferences. Although no future options are excluded, this type of marketing may have negative implications for individuals.

REFERENCES

Accenture. (2017). *Financial Providers: Transforming Distribution models for evolving customers*. Retrieved from Accenture: www.accenture.com/t20170111T041601__w__/us-en/_acnmedia/Accenture/next-gen-3/DandM-Global-Research-Study/Accenture-Financial-Services-Global-Distribution-Marketing-Consumer-Study.pdf

Accenture. (2019). *Global Financial Services Consumer Study.* Retrieved from Accenture: www.accenture.com/_acnmedia/PDF-95/Accenture-2019-Global-Financial-Services-Consumer-Study.pdf#zoom=50

Autoriteit Persoonsgegevens. (2019, July 1). *Compliancebrief.* Retrieved from Autoriteitpersoonsgegevens: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/compliancebrief_nvb.pdf

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2014). *Misplaced Confidences: Privacy and the Control Paradox, Social Psychological and Personality Science*. Pittsburgh: Sage Journals. Retrieved from Sage Journals.

Chrirkov, V., Ryan, R., & Sheldon, K. (2011). Human Autonomy in Cross-Cultural Context, Perspectives on the Psychology of Agency, Freedon and Well-Being. Dordrecht: Springer Science+Business Media. doi:10.1007/978-90-481-9667-8

Consumentenbond. (2019, June 17). *Goed rapportcijfers voor banken. ING blijft achter*. Retrieved from Consumentenbond: https://www.consumentenbond.nl/nieuws/2019/goede-rapportcijfers-banken.-ing-blijft-achter

Kerr, I., & Earle, J. (2013). *Prediction, Preemption, Presumption: How Big Data Threatens Big Picture*. Stanford: Stanford Law Review Online.

Levin, S. (2017, May 1). *Facebook told advertisers it can identify teens feeling "insecure" and "worthless"*. Retrieved from The Guardian: www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens

Moerel, L. (2014, March 1). *Big Data Protection: How to Make the Draft EU Regulation on Data Protection Future Proof*. Retrieved from SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3126164

Peppers, D., & Rogers, M. (2012). *Extreme Trust: Honesty as a Competitive Advantage*. New York: Penguin Group.

Wokke, A. (2014, March 14). *Instanties kritisch over proef ING met advertenties op basis van betalingsgedrag*. Retrieved from Tweakers: https://tweakers.net/nieuws/94841/instanties-kritisch-over-proef-ing-met-advertenties-op-basis-van-betalingsgedrag.html

Zuboff, S. (2019). *The Age of Surveillance Capitalism*. New York: Public Affairs.

ENDNOTE

[1] The study identifies three customer profiles, with different loyalty triggers, from which it can be deduced that the best starting position in competition is for financial service providers who are able to offer innovative digital services while maintaining a high level of customer service and trust (on acting in the interests of customers and protecting privacy). This is confirmed in (Accenture, 2019) (where four customer profiles have now been identified).