Privacy in Insurance: 3 sources of ethical risk for insurers

By Duncan Minty 31st October 2017

Privacy in insurance has been getting lots of attention recently, largely because of the imminent introduction of EU's General Data Protection Regulation. Yet there's a danger that this surge in legal and compliance activity will overly focus minds on the policy and process detail, while leaving scant time to think through the big issues that privacy in insurance raises.

It's important that insurers understand the big privacy issues that their business face, for a corporate privacy programme is only as good as the results it achieves on the outcomes that matter.

In this post, I'm going to look at three privacy concerns that insurers have to ensure that their privacy programmes are addressing. I'd recommend that these three privacy concerns be used to test just how robust those privacy programme are.

Aggregation

Aggregation involves the gathering and bringing together of data about a person from various different sources. The logic behind aggregation is that while a single piece of data here or there is not very informative, when several pieces are brought together, they begin to form a portrait of that person.

Why does the whole become greater than the sum of its parts in this way? It's largely down to data synergies. Aggregating data can reveal new facets of a person that she may not have expected to become known when she originally divulged each individual item of information in separate circumstances.

One may think then that if all this information had already been disclosed in one place or another, then bringing it together should not raise privacy concerns. Not quite. The public distinguishes between the scattered disclosure of pieces of information at various points in our lives, and the aggregation of it all in one place. We know that to live in an organised society we need to disclose information along the way, but we often feel uncomfortable when it starts being bundled together.

Why do we feel uncomfortable about this? The problem is that aggregated data can be informative, but it can also be misleading. The picture you put together about someone from scattered pieces of data may bear little resemblance to the real person. If you disconnect a piece of data from the context in which it was originally disclosed, there is a danger that it will be simplified, perhaps even distorted. That original disclosure could have been in a complex situation with quite different obligations and incentives to that of an insurance contract. Stripping away that context and attaching that piece of data to someone's record runs the risk of its meaning being contaminated.

Yet how does this differ from the situation up until now, in which policyholders have been obligated to disclose a wide range of data about themselves? It differs in two ways: firstly, there's a single, clear context (the insurance contract) in which disclosure is taking place, as opposed to a multiplicity of differing contexts. And secondly, data aggregation is invariably undertaken by computers according to a prescribed formula. This creates a rigid and unyielding process in which computerised information is accorded greater weight, and human interventions and interpretations become minimal. Data that might actually require substantial evaluation is instead reduced to discrete entries in pre-assigned categories.

To sum up. Data is not neutral. It's meaning relies heavily on the context in which it is disclosed (think of common phrases used in different ways). Ignoring that context can distort the meaning you try to draw from its aggregation.

Secondary Use

We all prefer to exercise some control over what information we divulge about ourselves and the uses to which that information is then put. This has less to do with any tendency towards secretiveness and more to do with an interest in ensuring that our information is put to use in ways that we're happy with. The privacy issue involved here is referred to as 'secondary use' and is one that the UK insurance sector has fallen foul of in the past.

Secondary use is the use of data for purposes unrelated to that for which it was initially collected, without the consent of the person involved. The public find secondary use troubling for a number of reasons. Firstly, when information is removed from the original context in which it was collected, it is more likely to be misunderstood or misconstrued. Such misunderstandings occur because someone disclosing a particular bit of information in one context for a purpose that fits that context may omit explanatory details that become crucial when that information is then used in another context. This is more common than we may at first think. We all tend to emphasise different aspects of a person or of an event, depending on the context in which we are discussing it.

Secondly, we are concerned about secondary use because it makes us feel uncertain about giving up our data in the first place. Not knowing how our data may be used in the future, or by whom, and not knowing how it may be misconstrued in a secondary context, can lead to feelings of insecurity and vulnerability.

And finally, it troubles us as a breach of trust, perhaps even of confidentiality, under the terms (formal or informal) to which we agreed the original disclosure. If a firm doesn't respect the terms under which the information was divulged to it by its clients, then it could well face questions about the trust its clients have in the products and services it provides. Trust isn't something the public applies selectively to what a firm gets up to.

An important feature of secondary use is the extent to which consent was sought, and then given, about the uses to which the information is to be put. If consent is to have any meaning, it has to be respected, be it in the context of medical, legal or financial services. Someone downplaying consent when designing an insurance process might want to consider how they would want their own clinical records handled in a medical context.

We all gain collectively from consent being respected and it is this which moves secondary use from being an issue about any one individual's information and turns it into an issue that's of concern to society as a whole.

Identification

Our personal identify is perhaps our most treasured possession. It defines who we are and reflects how we want others to see us. We expend much effort in developing this 'sense of being' and react defensively when we feel that it is under threat. For insurers, who we are and how we behave are at the heart of their underwriting process. This makes identification one of the key privacy issues that insurers need to attend to. It is however perhaps the most difficult one for insurers to get right.

Identification is the connecting of information to a particular person. It is something we all do throughout our lives, when we view others and others view us. It is also a constantly evolving activity, as we present different sides of our character to different audiences. So those aspects of our

identify we present to the prospective employer will not be the same as those we present to our friends in the pub that evening.

Does this mean that we are forever manipulating our identifies? Some who challenge privacy rights take it to be just that: a way of hiding what we don't want others to know about ourselves. They see this as a distortion of our identifies that can lead to distortions in market transactions, thus turning too great a concern for privacy into an impediment to efficient markets.

Like many privacy issues, there's clearly a balance to be struck here. On the one hand, our identifies are hugely multifaceted. That prospective employer may want to know as much as possible about us, but would almost certainly fall asleep before we were half way through it all. It's only natural that we select different aspects of ourselves for different audiences and keep some things private for only select friends. We want to be open, and private, and put our best front forward, as and when we choose. A vital part of our socialisation involves developing this skill, in large part by learning to read what others want of us.

On the other hand, manipulating our identifies to present unreal variants of ourselves to particular audiences can turn into fraud and should be treated as such. Deciding when such manipulation becomes fraudulent is ultimately for the courts to decide.

Remember that companies have identities too, which can be just as multifaceted as those of individuals. Public relations, marketing and communications departments work hard to present the best side of that identity to different corporate audiences, sometimes with genuine intent, sometimes not. Getting this right, and sustaining it over the long term, contributes hugely to what the company is worth.

Some aspects of our identity are so personal that we may in fact not want to disclose them to anyone. Indeed, we may not even want to find them out for ourselves. For example, the increasing ease of access to our genetic profile could raise such fundamental questions about who we are that some of us may prefer to remain ignorant about both it and its consequences. We can expect to be increasingly confronted with such choices as data becomes more prevalent, but in large measure, as a society we continue to allow such choices to be available. Whether businesses remain so tolerant is however less certain.

Many companies, such as retailers, banks and insurers, now have an identify of their own for you and are continually on the lookout for opportunities to extend it further. This is because the more they know about you, the more profitably they can market products and services to you. With 'big data' being seen as a significant competitive advantage, firms can sometimes be particularly determined to source ever more information about us. This raises the question of the firm's right to know versus our right to privacy.

Is there a limit to what a firm can find out about us? Can firms who want to feed ever increasing amounts of data into ever more sophisticated pricing models demand ever increasing levels of disclosure from us? It seems strange that in order for the firm to give us wider choice and more finely tuned pricing, we seem to have little choice but to acquiesce to such demands and activities. Some may say that the market will help find that balance between what one side wants to know and what the other side is willing to disclose, but in sectors like insurance, there isn't always a plethora of alternatives.

Our identities can also acquire quite peculiar characteristics under seemingly quite innocent circumstances. For example, policyholders who walk away from a claim without pursuing it fully are

now at risk of being classified as a probable fraudster, even though they only decided to do so after perhaps finding the excess too high or the repairs more easily managed by themselves. It is this danger of a somewhat warped version of our identities being secretly built up by the firms we do business with that seems to worry us the most.

So identification raises several ethical questions. They seem to add up to this: who decides who we are and who decides who gets to know about it.

Privacy in insurance is important. It's part of the relationship of trust between insurer and policyholder that sustains a healthy market. Insurers should use their knowledge of ethical issues such as aggregation, secondary use and identification to test their privacy programmes, to see that the response is in line with public concerns. After all, why go to all that effort for GDPR if you can't then use it in some way to build trust with consumers