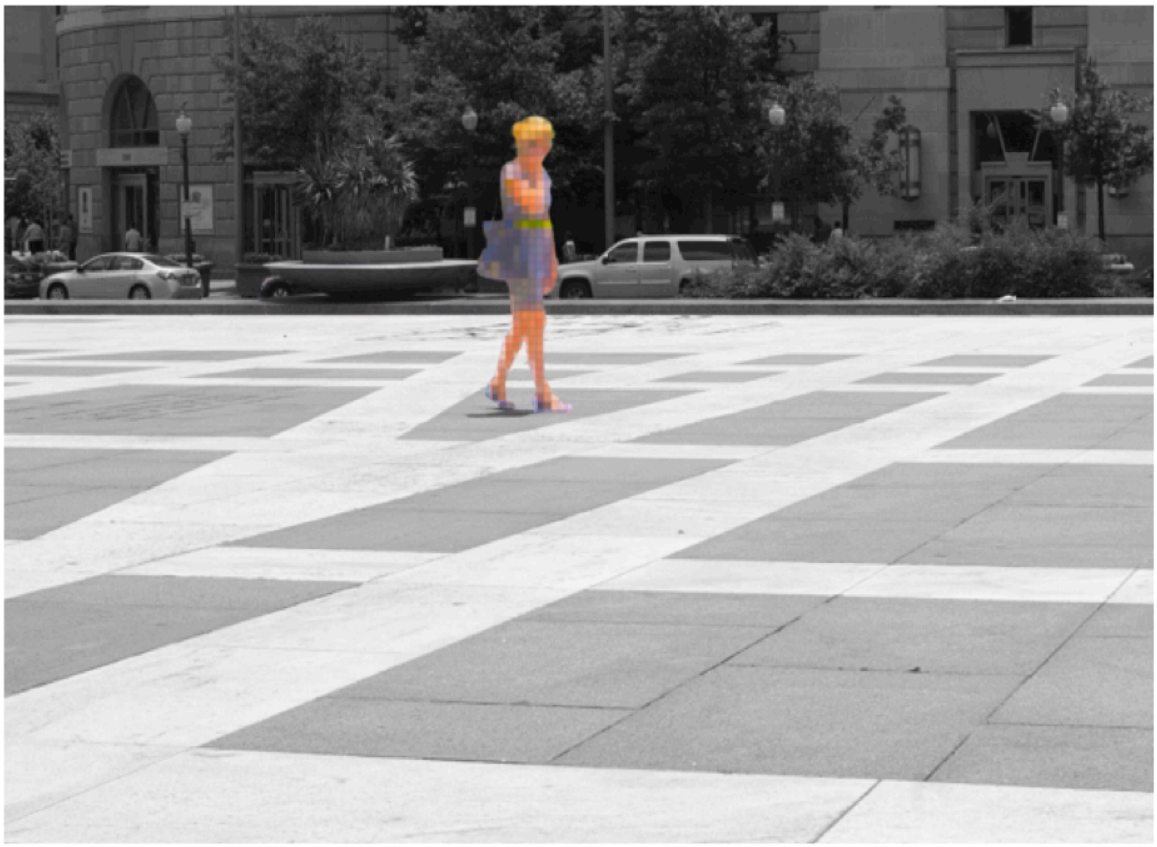

Ms. X in Freedom Plaza

Is Usage Based Insurance a Pathway to Greater Privacy, Not Less?

August, 2013

Corner Two Consulting

Colin Wright, Principal
colin@corner2.ca

Ms. X in Freedom Plaza

Is Usage Based Insurance a Pathway to Greater Privacy, Not Less?

While walking past Freedom Plaza during a recent trip to Washington DC I noticed "Ms. X" pacing about in the middle of the plaza fully engaged in a conversation on her mobile. Freedom Plaza is a large rectangular open space. It was a broiling hot day, the sun driving everyone but Ms. X from the plaza making her presence there remarkable.

Clearly, she had chosen the plaza because it afforded her privacy. With no one near, there was no risk of being overheard. Of course, there is no small irony attached to the fact that Ms. X sought to have a private conversation on a mobile phone in Washington's Freedom Plaza just as the whole Eric Snowden privacy/surveillance scandal was erupting. Sure, there was no one within earshot to actually overhear her end of the conversation, but we know with certainty that a record of her call exists. What we're less sure of is just how detailed that record might be and how such a record might be used.

> "Apart from foil hat-wearing conspiracy theorists, most people have come to accept that the benefits of our digital age can only be enjoyed if we are prepared to share some personal information."

Privacy, and, more particularly, its preservation and safeguarding are sensitive issues. The repeated, and often very public failures of governments and private enterprise to protect personal information cause varying levels of discomfort for people. Apart from foil hat-wearing conspiracy theorists, most people have come to accept that the benefits of our digital age can only be enjoyed if we are prepared to share some personal information. What is difficult to accept is that further innovation implies ever-greater risk to our privacy.

UBI – On the Vanguard of Enhanced Privacy

Services that we use daily can be surprisingly invasive. Google scans both the inbound and outbound emails of Gmail users searching for keywords that are then used to deliver paid advertising. Users cannot opt out of this practice. Over time, a profile of each user with detailed information based on their personal, private interests can be developed. Its search engine delivers even more personal data to Google. It's possible, or even likely, that Google knows things about users that they wouldn't want their closest friends to know.

Facebook, too, collects a wide array of personal data, and not just from users' 'likes'. Your life on Facebook affects your network of 'friends' because the responses generated through collection of your data are pushed out to those you're connected to. There are ways to opt out of this type of tracking and data collection but the default configuration supports the collection and use of significant amounts of personal data.

It's almost a given that to implement usage based insurance (UBI) will require mitigating the risk of negative effects on privacy because it is assumed that UBI will be similarly invasive to familiar online services. The position taken in this paper is that UBI actually provides an opportunity to enhance privacy – it can be, particularly over time, considerably less dependent on personal data than conventional auto insurance schemes. UBI can potentially upend the idea that digital innovation only comes with greater intrusion into our personal space.

The massive amounts of driving data collected by UBI programs diminish the need to use proxies based on more personal information to develop rates. It's conceivable that such programs will become increasingly indifferent to the characteristics of who is driving a vehicle by focusing almost exclusively on how, when and where the vehicle is being driven. The personal information required could boil down to little more than whatever is needed to render a bill.

Auto insurance, and the information needed for transactional purposes, could mirror the commercial relationships that typify other metered utilities. An electricity provider doesn't need to know your gender, marital relationships, household size, and so on, in order to manage its account with you. Generally, name, mailing address and payment preference are sufficient. Using a similar model, and despite having less personal information, a UBI customer relationship might be more intimate or more personally relevant than a conventional program allows. Through the use of web-based account dashboards to review usage and billing details, policyholders could gain some measure of control over their auto insurance expense and better appreciate how the data they provide may be used to their benefit.

"…despite having less personal information, a UBI customer relationship might be more intimate or more personally relevant…"

The real risk to personal privacy posed by UBI is unauthorized sharing and use of collected data. The challenge for policymakers, regulators, insurers and supporting businesses is to set privacy-enhancing boundaries, craft a set of workable rules and then to promote greater privacy as a benefit of UBI to policyholders. Now is the opportune time to dispel the notion that UBI means more intrusion. For an industry that is often regarded with suspicion by consumers, the advent of UBI is a chance to leverage technology for a more trusting, transparent and, ultimately more satisfying relationship.

Yesterday's Fear - "Big Brother is Watching"

Even before the Internet became a major commercial channel, it was understood that the price of access to goods and services was providing access to our personal data. As an example, the ease with which consumers can use credit products today rests on a virtual mountain of personal information gathered and analyzed over time. Friction is created in this relationship when the information is used for some purpose other than what is explicitly understood by consumers.

Insurance industry efforts to employ credit scores as a rating proxy spring to mind. Regardless of its utility when used for this purpose, many people view the practice as underhanded. Few would have understood at the time they surrendered it, that the information they provided when applying for a mortgage or credit card, or the information gathered surrounding their subsequent use of those products, would be used to price their insurance.

As usage based insurance (UBI) has been introduced in various markets an initial response has often been alarm about its potential to be invasive of privacy or that it has an Orwellian, "Big Brother" aspect. There is a fear that the information gathered will be used against consumers. This is not surprising; because of past events, alarm is the go-to response for many people with respect to any new process or technology that involves the electronic harvesting, storage, analysis and subsequent use of personal information.

A common rebuttal to these concerns is to suggest that "that train left the station long ago". The idea being that we are well past the tipping point where meaningful protection of information is possible, so we should simply decide whether or not the benefits offered by UBI outweigh the risks from a further erosion of privacy.

Personally, I find this argument difficult to set aside. I served as a juror for a criminal trial where my fellow jurors and I found the defendant guilty. Much of the evidence, and perhaps the most compelling, was comprised of the electronic trail left by the defendant. Mobile phone voice and text records, CCTV footage, credit card receipts, toll highway records, computer browsing history, etc., were all used to reconstruct events and implicate the accused. As our electronic lives become ever more integrated, the ability to reconstruct specific events in a person's life will become even easier.

No one can reasonably argue that UBI data could not, or will not, be used in this way. That doesn't mean that boundaries can't be established. Most people would probably support law enforcement agencies gaining access to UBI records under a warrant in support of a criminal investigation. They would, however, likely oppose the routine surrender of those records for the purpose of searching out potential speeding offenders.

UBI data is likely to be an attractive resource for policymakers as well. Again, rules are needed. UBI could, as an example, readily facilitate measuring and understanding road use across demographic groups or within specific geographies but if these data are to be used, the public might want to know that only aggregate data will be made available and that no submitted record will carry a personal identifier.

An overarching principle or test to be applied is that users must be able to demonstrate that their use of such information will serve the public interest. Of course, there are probably as many definitions of "public interest" as there are citizens. One way to approach the problem might be to limit the application of UBI data analysis to specific policy areas, such as highway safety or road use where there is likely to be some consensus on what constitutes the public interest.

Limits must be explored for insurers, too. It's a reasonable proposition that policyholders should be the "owners" of their driving data. They should be free to use that data to shop the market. They should also have the authority, in certain circumstances, to limit the use of their data. Today, a driver can choose not to report a single-vehicle accident where there is no loss or injury suffered by another party. If UBI data make it possible to identify such an accident policyholders should retain the right to choose whether or not to make a claim. There is potentially a reciprocal benefit for insurers if it is established that they have the right to analyze UBI data to help determine the legitimacy or fraudulence of a claim.

"It's a reasonable proposition that policyholders should be the "owners" of their driving data."

With UBI in its nascency in Canada, it is an opportune time to establish appropriate boundaries. As with other aspects of UBI, it would be preferable to set the rules and mark out the playing area before the participants take to the field.

Contracts, Implied and Otherwise

Computer scientist and virtual reality pioneer, Jaron Lanier, argues that one of the problems inherent to digital business models is that the relationship is decidedly one-sided. Lanier notes that, "Ordinary people are relentlessly spied on, and not compensated for information taken from them."[1] It is no secret that the Facebooks, Googles, Apples and LinkedIns of this world make money not only by leveraging the information willingly surrendered by users, but also by using the data users provide unwittingly through their use of these products or services. It's reasonable to believe that it is the intention of the operators of almost any site where you are asked to provide personal data to treat that submission as a licence to gather additional information about you through your use of their product.

Anyone deciding to access almost any online service is accustomed to being asked to grant their permission by reading and accepting a set of terms and conditions. Most of us scroll to the bottom of the pages-long Ts & Cs and hit "I Agree" without a second thought. And, while it is fair to argue that we should actually *read* what it is we're agreeing to, this approach is really a bit of a subterfuge. While it probably satisfies legal necessity, it trades on our common aversion to wading through sentence after sentence of craftily, or at least confusingly worded text before being allowed to play with this week's new toy.

There are two problems in all of this: we've entered into a lopsided agreement where we're surrendering something of value without any promise of compensation, and; we don't know what we've agreed to. Lanier argues that, "In a world of digital dignity, each individual will be the commercial owner of any data that can be measured from that person's state or behavior." He further adds, "In the event that something a person says or does contributes even minutely to a database that allows, say, a machine language translation algorithm, or a market prediction algorithm, to perform a task, then a nanopayment, proportional *both* to the degree of contribution *and* the resultant value, will be due to the person."

Which brings us to the agreement between insurers offering UBI and the policyholders who plug in a device and authorize the use of their driving data for ratemaking. In very simple terms, the policyholder is exchanging access to their data for the possibility of compensation in the form of merit-based premium discounts or, at a minimum, the least punitive rate possible. The terms of the transaction are straightforward and are typically highlighted in product marketing materials. In this respect, UBI addresses Lanier's concern that individuals are compensated for the use of their data.

This is an interesting agreement because one party, the service provider, is asking the other to knowingly be placed under surveillance in exchange for potential benefit. This is unlike other services where the subscriber may not readily understand that their activity will be surveyed, they have no knowledge, or limited knowledge of how the gathered data will be used, and there is no offer of compensation for the use of their data.

Proposal – Some Guiding Principles

Secondary use of UBI data is where there may be a privacy concern. As noted previously, there are myriad uses that UBI data could serve, some of which might well be in the public interest and so it probably makes sense to provide some form of access to third parties. Possible guiding principles could include, but not be limited to, the following:

1. Only aggregate data may be shared with third parties except in the case of a criminal investigation;
2. Individual data records must be stripped of all personal identifiers;
3. Notification of what data will be shared and the purpose of its proposed use must be provided in advance to policyholders (policyholders could grant permission for specified uses when they initially sign up for UBI);
4. Individual policyholders are entitled to a fair share of any compensation paid for access to their aggregated data (in effect, this may be a symbolic gesture, but nonetheless an important principle).

In brief, when someone contracts for UBI they should understand that: they will be "spied upon" within agreed to limits; they have the opportunity to receive financial consideration for the data collected from them; their data will only be shared with third parties in aggregate and only with their consent; they will receive a representative share of any compensation paid for use by third parties; and they will own their data.

UBI is Inherently Less Invasive of Privacy Than Conventional Underwriting

Progressive Insurance, which has been developing its UBI offering for more than a decade, used the "Big Brother" concern to its advantage. As it expanded its offering state-by-state, Progressive would use press releases and other public relations efforts to generate interest in the product. In a conversation I had with Progressive's general manager for usage based insurance, Richard Hutchinson, several years ago, he noted that where insurance news generally garnered little interest, the combination of insurance with telematics technology did catch the eye of the media. Typically, they were interested in how the product worked, but were also quick to seize on the idea that policyholders were being spied on.

I like to think of this as a benign controversy, and savvy marketing, because although the media's premise was negative the outcome was consumer awareness and sales for Progressive's UBI product at a time when the company was not prepared to support it with a significant marketing budget. Hutchinson and other company spokespeople highlighted that their product did not use location data and that most policyholders received meaningful premium discounts in exchange for their data, which most saw as a fair trade-off for any real or imagined loss of privacy.

As UBI is rolled out in Canada, the same questions and concerns around privacy surface in the media. When Desjardins rolled out its *ajusto* product this past spring, reports on the CBC included expressions of concern over the "invasive" nature of such programs.[2] The coverage from other media outlets is unlikely to take a very different tack. Like Progressive, Desjardins has highlighted the benefits available to its *ajusto* clients rather than attempting to push back very hard on the underlying assumption that UBI *is* more invasive.

But is it, or does it have to be? The answer is, no. In fact, UBI can be less invasive. Industrial Alliance's *Mobiliz* program illustrates how this can be so by not even requiring that applicants divulge their past claims history. Today, to obtain a quote for a conventional auto policy, drivers must surrender considerable personal data: age, gender, years licensed, claims history, driving record, occupation, marital status, current policy information, what the primary use of the vehicle is, and so on. Insurers would use credit ratings if permitted. If you add your university-attending son or daughter to the policy you may be asked to indicate if they live away from home during the school year and what school they attend. The distance from home of their school is used to decide whether a discount can be applied for their expected limited use of the vehicle while away at school.

That's a lot of information, and much of it could become superfluous to needs as UBI expands into the marketplace meaning that UBI, rather than posing a threat, has the potential to increase privacy and be less invasive. By ignoring past claims history, and even claims made under the policy, the *Mobiliz* model is emphasizing that what really matters is your current vehicle use and driving behaviour. Extending that forward, as more data is collected and understanding of what drives losses increases, insurers may become less and less concerned with personal details; they will need to know less about who is driving the car because they will know all they need to know about how it is being driven.

In the past, repetition and examination of the "Big Brother" meme by the media may have served the industry's interests by generating awareness for what was generally a niche product. That may be less the case today. Broader, technology-related privacy concerns may actually hinder adoption of what is rapidly becoming a mainstream product offering. The industry should work with policymakers and regulators to create a robust privacy framework and also work to promote the idea that trip details are far less personal in nature than some of the data gathered for use as

> "Controlling who shares your data is no different than trying to prevent someone eavesdropping on your conversations."

proxies today. Insurers should highlight that, apart from offering more fair and equitable rates to drivers, an important benefit of UBI will be a much reduced requirement to gather personal information and, therefore, greater privacy, not less.

Back to Freedom Plaza

Presumably, Ms. X achieved her aim and avoided having anyone eavesdrop on her call. In all probability the detail of that conversation has been lost to the ether although the record of its occurrence, the number of the other party and Ms. X's location at the time of the call are likely still retrievable.

When cellular technology started to become commercially available thirty years ago it's unlikely that anyone anticipated how it would evolve and how readily it would lend itself to providing a trove of information about users. And let's face it, most of us love how we can find our favourite coffee shop, effect transactions and keep track of our family and friends in real time; we've fallen again and again as more and more capability is delivered in ever more seductive packaging.

Perhaps because the technology and the services it enables evolved rapidly over a short time frame, most of us didn't give a second thought to how else it could be put to use and how that might impinge on our privacy. With UBI, though, we have a better understanding of how the enabling technology works and why it's important to include the protection, or even enhancement of privacy among our objectives for it as it's being brought to market. Controlling who shares your data is no different than trying to prevent someone eavesdropping on your conversations. Consumers have a right to expect privacy; unlike Ms. X they shouldn't have to actively seek it.

---

[1] Lanier, Jaron, *Who Owns the Future?,* Simon & Schuster, New York, 2013.
[2] See: http://www.cbc.ca/player/News/Canada/ID/2389935240/ or http://www.cbc.ca/news/yourcommunity/2013/06/readers-hit-the-brakes-on-car-insurance-trackers.html