White Paper

Information Privacy: Carriers Need to Be Savvy, Loud & Proud

Prepared by

Patrick Donegan
Senior Analyst, *Heavy Reading*
www.heavyreading.com

on behalf of

CLOUDMARK®

July 2014

Executive Summary

The so-called Snowden revelations have permanently altered the global ICT landscape. While the Googles and Facebooks of this world have responded loudly and strongly, the response of telcos thus far has been comparatively meek. This white paper looks at how telcos and leading over-the-top (OTT) players are adjusting to the Post-Snowden era, what's at stake and what the operators need to do to reinforce their competitive positioning in regards to user privacy. Ironically, one of the things the operators must do is ensure that key aspects of their security and privacy strategies are fully aligned.

Information Security in the Post-Snowden Era

In May 2013, volumes of classified information concerning the activities of America's National Security Agency (NSA) in monitoring the world's communications networks were exposed to the UK's "The Guardian" newspaper by former NSA contractor, Edward Snowden.

The so-called "Snowden Revelations" shone an unprecedented light on the scale of the U.S. government's infrastructure for monitoring and accessing global databases and global information flows. They triggered a huge uptick in public debate in many countries throughout the world about the appropriate balance between the rights of the citizen and those of the government when it comes to the security of an individual's private information, whether that be in regards to their data storage, social network postings, voice, data or messaging communications.

The Outrage of the Internet Giants

The segment of the telecom value chain that has been most vocal in supporting the rights of consumers to be concerned – even outraged – about the Snowden revelations have been the Internet Giants, known to telcos the world over as OTT providers.

In December 2013, eight of the world's leading technology companies announced the formation of an alliance called the Reform Government Surveillance group. The eight companies are Google, Apple, Facebook, Twitter, AOL, Microsoft, LinkedIn and Yahoo. The group's mission statement includes the following:

> *"The undersigned companies believe that it is time for the world's governments to address the practices and laws regulating government surveillance of individuals and access to their information. Consistent with established global norms of free expression and privacy and with the goals of ensuring that government law enforcement and intelligence efforts are rule-bound, narrowly tailored, transparent, and subject to oversight, we hereby call on governments to endorse the following principles and enact reforms that would put these principles into action."*

Several leading CEOs from these companies provided additional supporting statements to reinforce their commitment to the Reform Government Surveillance agenda, including the following:

- "The security of users' data is critical, which is why we've invested so much in encryption and fight for transparency around government requests for information. This is undermined by the apparent wholesale collection of data, in secret and without independent oversight, by many governments around the world." – **Larry Page, CEO, Google**.

- "Reports about government surveillance have shown there is a real need for greater disclosure and new limits on how governments collect information." – **Mark Zuckerberg, CEO, Facebook**.

Many of these companies are carrying out a high profile media offensive on this issue. And they are supporting with development commitments to introduce

superior encryption techniques designed to thwart universal or dragnet monitoring techniques of the kind that Edward Snowden alleges have been used by the NSA.

With the exception of a minority of people who might be wholly wedded to the idea of authoritarian government, the above are principles for which the large majority of human beings would gladly sign up. To put it another way, what's not to like about them?

Well there is one thing: They only address the potential for misuse or abuse of private information by one actor in the online value chain, namely the government. The reality, however, is that in today's online environment private information can be vulnerable to abuse or misuse by a variety of other actors. Indeed the entire business models of some of the Internet companies is based on exploiting peoples' private information in ways that are insufficiently transparent, provide too little user control or provide inadequate compensation for many peoples' liking. Hence the aggressive lobbying against excessive oversight by the government does leave the Internet giants vulnerable to charges of hypocrisy.

The Post-Snowden Era in All Its Aspects

In public and industry discussions of user privacy over the last twelve months, the term "Post-Snowden Era" has started to morph from its original meaning relating to large scale NSA monitoring of global communications. It has become a much broader umbrella term for public concern about an individual's vulnerability to abuse of their digital lives by businesses, hackers and fraudsters, malicious strangers and malicious former-friends and partners, as well as by governments.

Figure 1: Consumer Research Shows Growing Internet Privacy Concerns

SURVEY ORGANIZATION	DATE & SAMPLE (COUNTRY)	SURVEY FINDINGS
ComRes*	**02/2013** *10,354* (8 major international markets)	79% are concerned about their privacy online. 41% say they are being harmed by big companies gathering large amounts of personal data for internal use. 65% believe national regulators should do more to force compliance with existing regulations concerning online privacy and the protection of personal data.
Pew Research Center	**7/2013** *792* (US)	68% believe current laws are not good enough in protecting people's privacy online. And 50% are worried about the amount of their personal information that is online – up from 33% in 2009.
Harris for ESET	**11/2013** *2,000* (US)	19% of consumers are banking less online and 14% are cutting back their online shopping.
Hart Research **	**11/2013** *558* (US)	43% of teens say they are "very concerned" about online privacy, up from 35% a year ago.
Benenson Strategy Group ***	**12/2013** *1,000 voters* (US)	80% more worry their information will be hacked to harm or steal from them, while only 16% worry that their personal online information will be used by companies to target advertising to them.
Global/WebIndex	**01/2014** *170,000* (global)	56% worry about the Internet eroding their personal privacy, up from 50% two years ago.
Ipsos Mori	**01/2014** *2,000* (UK)	60% more are concerned about online privacy compared to a year ago.
Harris Interactive (for Truste)	**01/2014** *2,000* (US)	74% of Internet users are more worried about privacy than a year ago.

* Germany, UK, France, Spain, Brazil Australia, Japan, India, S. Korea
** For Family Online Safety Institute
*** Benenson and American Viewpoint for the Computer & Communications Industry Association (CCIA)

Source: Heavy Reading

For example, many people are concerned about the following:

- The commercial exploitation of an individual's online behavior for commercial purpose by bona fide businesses, both in cases where the individual does not authorize such exploitation, as well as where they do.

- The growing volume and sophistication of cyber-attacks that target a person's private information – either to delete that information, make money by selling it or leverage it to steal money directly.
- The readiness of individuals to voluntarily expose so much personal information on social networking sites in ways that renders them vulnerable to so many different kinds of abuse or indeed vulnerable to criminal prosecution.
- The exploitation of an individual's online behavior for commercial purpose by bona fide businesses, both in cases where the individual does not authorize such exploitation, as well as where they do.
- The lag in law making and law enforcement in regards to privacy and libel between the online environment and more traditional media.
- The vulnerability of unsupervised children to the same hazards as adults in their online lives, albeit with a much less-developed emotional ability to cope when things go wrong.
- The potential intrusiveness of new user technology such as Google Glass.

Concerns such as these are at least as great in the minds of consumers as the risk of unwarranted spying on their private affairs by government. In fact, as shown in **Figure 2**, a Kaspersky Lab survey of 8,605 consumers from all over the world published in August 2013 suggests that consumers are substantially more afraid of their information being stolen by other people or misused by businesses with whom they share their information than they are of having their data misused by government

Figure 2: The Private Sector Poses a Greater Privacy Threat Than Government

Source: Kaspersky Labs, August 2013 # 8605

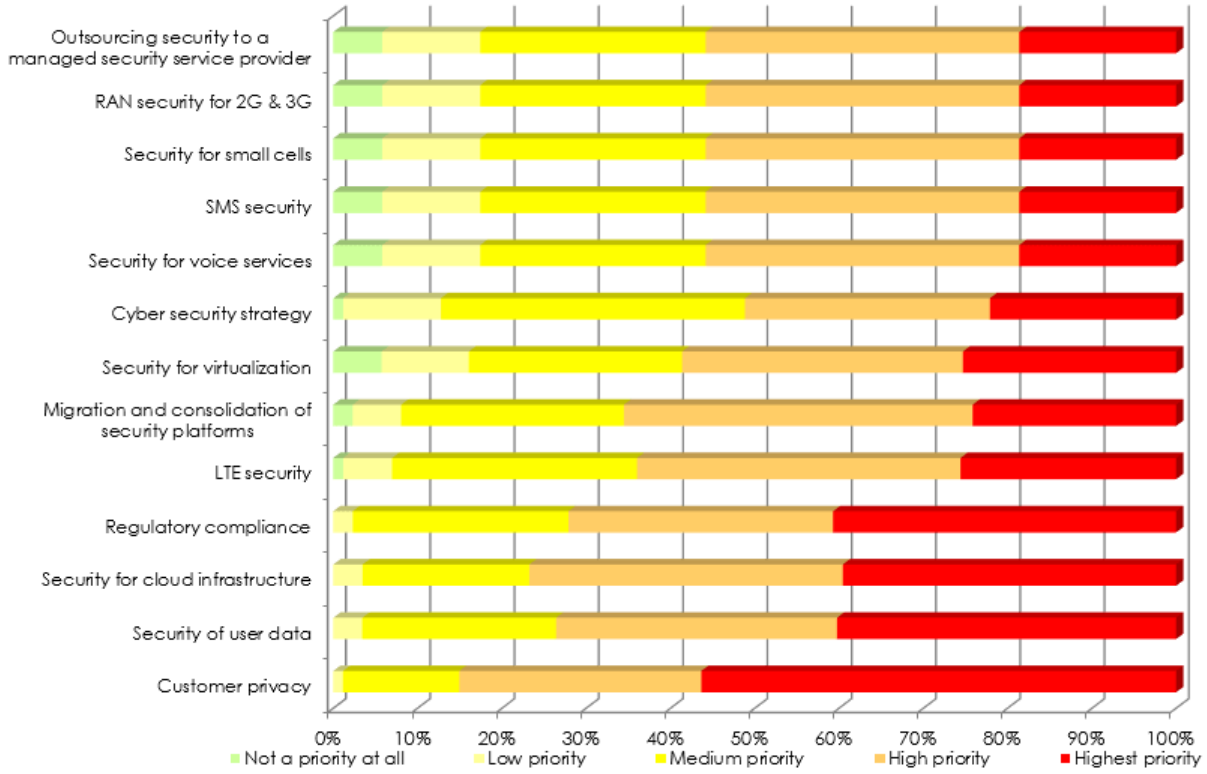
As shown by some of the research evidence cited in **Figure 1**, concern about vulnerability at the hands of other market actors besides government existed long before the Snowden Revelations came to light. However, concerns have clearly become heightened over the last year. It is difficult to prove a direct causal link, but the extensive media coverage of the Snowden Revelations over the last 12 months makes it likely that they have increased consumer awareness and anxiety about the full gamut of threats to personal information, whether they come from government, businesses, individuals operating within the law or criminals breaking the law.

Privacy Anxiety: Implications for Carriers

Information privacy matters, whether that be in regards to data storage, social network postings, voice, data or messaging communications. At the point of sale, and in analysis of subscriber churn, privacy still doesn't rank as high as price, coverage and performance. Moreover, its importance is evolving in different ways and at different rates in different countries based on different cultural and political factors. But as shown in **Figure 1** there is no doubt that at an aggregate level online privacy is growing in importance.

Telcos get this. As discussed further on, information privacy always has been, and remains, an integral part of the DNA of telco culture. So much so, that today information privacy should be considered a competitive advantage for telcos. Except where government issues a specific Legal Intercept order, which they are legally bound to comply with, for the most part telco business models have traditionally revolved around protecting subscriber information. By contrast the business models of the Internet companies tends to revolve around capturing and monetizing subscriber information and/or encouraging them people to publish it on the global Internet.

Figure 3: Customer Privacy Is the #1 Security Issue for Mobile Operators



Source: Heavy Reading

Heavy Reading's own research demonstrates how seriously telcos continue to take information privacy. In **Figure 3** (above), for example, a survey sample of 66 mobile operator respondents conducted in September 2013 overwhelmingly nominated

customer privacy as their company's highest security priority in the coming 12 month period. As Håkan Kvarnström, chief security officer at TeliaSonera AB, told *Light Reading* in April 2014, "Of course, it's serious if the network goes down, but that's reversible – we can do something about it. That's not as far-reaching as losing data."

As telcos prepare to design service, product and marketing communications (marcomms) strategies in the Post-Snowden era, there are several new risks that must be navigated. These consist of a risk to overall consumer demand from privacy anxiety, as well as a risk to both the revenue model and the competitive landscape.

Risks to Overall Consumer Demand

While it may be partially true that many consumers still aren't all that bothered about some aspects of privacy, **any factor that deters consumption of Internet services and applications by any of its customers is bad for carriers**. As Stephen Deadman, group privacy officer at Vodafone, put it in an Interview with the Guardian newspaper in January 2014: "We want all of our customers worldwide to feel they are at liberty to communicate with each other as they see fit. We want our networks to be big and busy with people who are confident they can communicate with each other freely; anything that inhibits that is very bad for any commercial operator."

The way that carriers address the issue of privacy will become more of a differentiator as they compete with one another in the coming years. As long ago as in May 2012, Randall Stephenson, chairman of AT&T, commenting on future opportunities in the mobile internet, stated that "the long pole in the tent is going to be getting the ecosystem to be robust in protecting data and making sure you control who sees the data, how it's shared and how its transmitted. Getting that right will enable [this market] to explode. Until you get it right there is going to be inherent apprehension and concern by all of us about this."

Risks in the Competitive Landscape & to Emerging Business Models

As already shown, the CEOs of the major Internet technology companies are aggressively positioning themselves as the consumers' champion in regards to protecting their online privacy. This poses some form of competitive threat to carriers. Specific carriers each have unique relationships with specific Internet companies and these relationships come in infinite shapes and sizes. However, there is an aspect of these relationships that is competitive in terms of each party's quest for the largest possible share of the same subscriber's brand loyalty and expenditure. Since the Internet companies are upping their game on user privacy with their CEOs making headline-grabbing public statements championing the cause of user privacy, the power of the media to shape peoples' attitudes, being what it is, the telcos should be very wary of allowing them to occupy that moral high ground unchallenged.

Telcos know that better leveraging subscriber information for themselves is one of the critical things they must do to arrest the decline in their revenue performance. But if they don't do this at least somewhat differently than the Internet companies do things, consumers that care about privacy will conclude that telcos are "just as bad." This would risk the competitive advantage that the telcos now enjoy over the Internet companies being eroded.

Today's Telco Privacy Strategies

It's worth remembering what telcos already do today to protect their subscriber's privacy and that subscribers are already seeing the benefits of.

- They invest in technology and operational processes to protect subscriber databases against theft of information either from rogue insiders or external attackers.
- They invest in network security to protect against short message service (SMS) and email spam and malware designed to steal subscriber information from making its way onto the end devices of subscribers.
- They invest in user education to provide guidance with respect to good phone, PC and smartphone hygiene that can prevent information leakage.
- They provide encryption at various points in the network to protect voice and data traffic against illegal interception.
- They work with ecosystem partners in the applications and devices arena to minimize the risk of rogue applications and operating system vulnerabilities making their way into the network and compromising subscriber information.
- They disclose information to government and police authorities only in specific instances where they are required to by law.

Behind the scenes most telcos are also working very closely with industry associations, national and multi-national regulators on information privacy issues. They are working on blueprints and legislation to enable optimal compromises and a level playing field for industry in terms of the balance between the very real benefits to be gained from extending the role of "Big Data" in economies and societies, while also enhancing security, choice and control for individual consumers with respect to their information privacy.

Next Steps in Carrier Privacy Strategies

Telcos have always understood information privacy, and they still understand it today. For the most part they also "get" that the Snowden revelations have changed the landscape in information forever.

Ironically, the one part that these providers of communications services have yet to fully understand and respond to is the need for them to begin communicating around the subject of information privacy. Not just communication to customers in the sense of mobile phone hygiene advise or malware protection that can be viewed or downloaded from their home page, but, rather, they need to communicate opinions and articulate visions in the local news, as well as global media outlets that are giving such a high profile to the privacy-related proclamations of Facebook, Google, etc.

This is certainly a challenging proposition for CEOs and CMOs to get their heads around. As previously stated, privacy still isn't a top-of-mind issue for most customers at the point of sale. Being regulated companies under license from governments, it has always been in the nature of anything related to telco security that privacy is typically discussed behind closed doors, rarely in public, and only then in policy forums and by security experts and lawyers.

And if the weight of tradition and the lack of real urgency from many consumers isn't enough to deter CEOs from getting their megaphones out to compete with Larry Page and Mark Zuckerberg, then the fear of alienating these Titans of the Internet or making bold privacy commitments today that they may not be able to live up to three years hence probably is.

An Old Mindset That Must Be Overhauled

Since the Post-Snowden era clearly marks a break with the past the telco mindset regarding security needs to shift accordingly. The Internet companies have moved first, focusing on the issue of government surveillance. That's certainly not a red herring, but it's also not the biggest risk to most subscribers from within the family of Post-Snowden risks to privacy.

The CEOs of the Internet companies might not be dominating the detailed policy discussions behind closed doors and in detailed policy for a, but they are dominating media headlines and steering the public debate to a direction of their choice virtually unchallenged by their telco counterparts.

Some of the factors preventing the telcos from responding are more important than others. Differentiating themselves from the Internet companies in the way that they leverage subscriber information without making unrealistic commitments is among the most challenging. Fear of alienating the Internet companies is arguably less so.

Just how willing are the Internet companies to offer significantly favorable deals to one carrier rather than another (Apple excepted)? And just how heavily would a few barbed media comments really weigh on deal negotiations, especially if those comments are anonymized rather than targeted at one specific company? The etiquette of a 1920s gentleman's club isn't expected in Silicon Valley in 2014. If anything, it's more likely to inspire derision.

Guiding Principles of a Post Snowden Privacy Communications Strategy

So what should a telco communications strategy for privacy look like in the modern era? Here are some suggestions:

- **Communicate to subscribers what the company is already doing for them to protect their privacy.** Short items of information – maybe even text messages –will have value in enhancing perceptions of the telco as the user's defender against the types of online invasions of privacy that matter most to end users. Examples could be information about the ways in which their information is (and isn't) currently used; use of encryption in the network; the use of message filtering and malware protection; or even company policy with respect to Legal Intercept.
- **Build specific value propositions and guarantees around information privacy.** Besides just offering anti-virus clients, telcos should make specific commitments such as compensating users for any malicious messages that they receive.
- **Bring out the CEOs**. The diligent efforts of middle ranking executives in devising and promoting detailed privacy strategies are critical in influencing colleagues, regulators and industry partners. The same can be said of industry associations. But to influence consumers directly with ideas about a company's differentiators in the privacy domain there is no substitute for the CEO directly addressing these issues in the media.

Recent Examples of Telcos Showing the Way

- **Vodafone Group plc** has stated it will be requesting from the UK government, and the governments of each of the 25 countries in which it operates, the right to disclose the number of demands it receives for wiretapping and customer data. Vodafone would like to disclose surveillance requests in its annual sustainability report, due to be published in June.
- **BT Group plc CEO Gavin Patterson** has publicly commented on the issues thrown open by the Snowden revelations, stating: "It's just too murky at the moment. It needs to be transparent and [there] needs to be clear guidelines about what's acceptable and what isn't," adding that the legislation has to "catch up" with the real world.
- **Deutsche Telekom** issued a press release in December 2013 announcing the introduction of the A5/3 encryption algorithm into its GSM network to succeed the original A5/1 that is now considered to be potentially vulnerable. Thomas Kremer, the DT Board member responsible for data privacy, legal affairs and compliance stated: "We are doing all we can to provide better security for our customers. Improved encryption of mobile phone conversations is another important step in this direction."
- **Bell Canada offers customers compensation for receiving rogue messages.** For $5 a month, Bell Canada customers can subscribe to a service whereby they are provided with a refund for any rogue messages they receive.

Security & Privacy Don't Align Automatically

As shown, leading operators are having to turn their attention to the privacy associated with each and every aspect of the service they provide to their customers. Doing so will not just ensure that they comply with regulations, but will also provide them with a platform from which to create competitive differentiation for themselves and a benchmark against which to rank themselves against non-telco competitors.

Ironically, if they want to really turn up the heat on their non-telco competitors in regards to privacy, one area operators need to look at pressing home their advantage is their own network security policies, specifically their own messaging security solutions. Personal privacy and broader security objectives don't just need to be approximately aligned. For privacy to be elevated to the highest possible customer value proposition in the post-Snowden era, the alignment needs to be as near-perfect as possible. And in an era when "Big Data" also represents a major revenue opportunity for all market actors in the value chain, a near perfect alignment cannot be taken for granted.

In the messaging domain there are several questions that operators must ask themselves about the message filtering solutions they put in their network to ensure that their security and privacy strategies are properly aligned:

- **Are suspicious messages being queried and treated internally within the operator's own network or are they being sent off-net to a third-party scrubbing center?** If they are going off-net, what guarantees does the operator have that the third party complies with the same national and international data protection standards as the operator itself?
- **How susceptible is a suspicious message to human intervention within the messaging security architecture?** To what extent can the data generated about a suspicious message be fully anonymized so that the message content cannot be correlated with Personally Identifiable Information (PII), such as email addresses, domains and IP addresses, in a way that would compromise customer privacy?
- **Can threat-related information associated with specific messages – rather than the actual user content of the messages – be reported into a threat center?** Can this be done in a way that is anonymized and protects the privacy of the sender or recipient of the message? And where users would be willing to opt into an operator's messaging abuse reporting service but local privacy regulations restrict the ways in which this can be done, can the operator's messaging security solution support that?

Summary & Conclusions

Respect for subscriber information has been a key differentiator for telecom operators, going back several decades. In the post-Snowden era, however, the Internet giants have made a head start in positioning themselves as the consumer's champion against just one of many types of intrusion on individual privacy.

As telcos look to compete for customer loyalty and customer wallet share with these same Internet companies, they need to get onto the front foot where customer privacy is concerned. That requires a more aggressive communication strategy led at CEO level, supported by a still greater prioritization of privacy in all aspects of the operator's business model, including its security strategy.

Background to This Paper

About Cloudmark

Given the breadth and complexity of today's messaging attacks, service providers need a scalable and targeted messaging security solution to protect their networks. Cloudmark's carrier-grade solutions simplify and advance the management of messaging abuse, while increasing utilization and reducing infrastructure costs.

Cloudmark works with operators across the globe to help ensure their networks are secure, while also providing their subscribers with the highest level of security and privacy around their messaging experience. Cloudmark enables operators to take control of their messaging environments by delivering a solution that won't compromise user privacy. With Cloudmark, telcos and their subscribers are protected against the latest messaging threats with the company's renowned team of security experts and its continuous research and innovation.