WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Personal Data: The Emergence of a New Asset Class

Opportunities for the Telecommunications Industry

An Initiative of the World Economic Forum
February 2011

In Collaboration with Bain & Company, Inc.

This paper reflects a subset of the discussions with experts and stakeholders in the context of the “Rethinking Personal Data” project.

For a more comprehensive overview of the results of this project please refer to the public report “Personal Data: The Emergence of a New Asset Class” by the World Economic Forum, available at http://www.weforum.org/personaldata.

Title picture by frog design inc.

Acknowledgements

This document was prepared by the World Economic Forum, in partnership with the individuals and organisations listed below.

World Economic Forum

Professor Klaus Schwab	Executive Chairman
Alan Marcus	Senior Director, IT & Telecommunications Industries
Justin Rico Oyola	Associate Director and Project Lead, Telecommunications Industry
William Hoffman	Head, Telecommunications Industry

Bain & Company, Inc.

Michele Luzi	Director

The following experts contributed substantial research and interviews throughout the “Rethinking Personal Data” project. We extend our sincere gratitude to all of them.

Julius Akinyemi	MIT
Alberto Calero	France Telecom
Ron Carpinella	Equifax
Chris Conley	ACLU
Douglas Dabérius	Nokia Siemens Networks
Timothy Edgar	Office of the Director of National Intelligence, USA
Jamie Ferguson	Kaiser Permanente
Michael Fertik	ReputationDefender
Tal Givoly	Amdocs
Kaliya Hamlin	Personal Data Ecosystem
William Heath	Mydex
Trevor Hughes	International Association of Privacy Professionals
Betsy Masiello	Google
Mita Mitra	BT Group
Drummond Reed	Information Card Foundation
Nasrin Rezai	Cisco
Natsuhiko Sakimura	OpenID Foundation
Kevin Stanton	MasterCard Advisors
Pamela Warren	McAfee
Von Wright	AT&T

Project Steering Board

This work would also not have been possible without the commitment of:

John Clippinger	Berkman Center for Internet and Society, Harvard University
Scott David	K&L Gates
Marc Davis	Microsoft
Robert Fabricant	frog design
Philip Laidler	STL Partners
Alexander (Sandy) Pentland	MIT
Fabio Sergio	frog design
Simon Torrance	STL Partners

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Executive Summary

Personal data – that growing trove of digital data created by and about people – represents untold opportunities for economic growth and societal good.

Existing in silos across cyberspace, it includes everything from our personal profiles and demographic information to bank accounts, medical records and employment data. Increasing in volume from the rapid uptake of new mobile devices, social technologies and sensors, it also includes our digital lives. All of our Web searches, site visits, purchases, tweets, texts, emails, phone calls, photos, videos and even the coordinates of our real-world locations are housed in databases around the world.

Some consider personal data to be the new "currency" of the digital economy. But even as it rapidly emerges as a new asset class that touches all aspects of society, its future is unclear. It is an ecosystem of unprecedented complexity, velocity and global scale. Most importantly, it demands a new way of thinking about the central importance of the individual.

"Personal data is the new oil of the Internet and the new currency of the digital world."

Meglena Kuneva, European Consumer Commissioner, March 2009

It was in this context that the World Economic Forum launched its "Rethinking Personal Data" project in 2010. This multiyear effort strives to capture the best thinking about the evolution of a personal data ecosystem from the perspectives of such diverse stakeholders as private companies, public sector representatives, end-user privacy and rights groups, academics and topic experts. The project's overriding belief is that such an ecosystem must benefit all – and therefore requires active engagement to ensure that every stakeholder benefits.

Telecommunications firms are a core constituency within the project. Focused on identifying breakthrough strategic growth opportunities, the telecommunications sector is well positioned to participate in the personal data opportunity. Possessing competencies and assets that can be effectively brought to bear, telecommunications firms have access to highly specific user location information, the ability securely to manage high volumes of data and the ability to identify and authenticate individuals on a massive scale. Also of unique value is the brand trust that individuals have for communications service providers (CSPs).

As the pressure mounts for CSPs to innovate and unlock new revenue sources, the need to explore personal data's opportunities fully cannot be dismissed. Indeed, estimates for just two potential CSP personal data services – the identification and authentication of users of third-party services and offerings to profile and target customers for individualised advertising – are estimated to be worth US$52 billion in revenues within the next 10 years in the US and Europe.[1]

[1] Estimates by STL Partners, 2011.

Pursuing these opportunities, however, is not without risk. Telecom firms today face multiple challenges. In the privacy realm, these range from meeting legal liabilities in managing personal data to loss of user trust as a result of privacy breaches. Beyond that, gearing up entails uncertain business models and massive initial investments without clear, short-term revenue returns. With many competing demands on their resources, many operators are reluctant to make investments in personal data services a priority.

The risks inherent in rapid innovation only add to the complexity. A number surfaced in discussions with telecom strategists. First, in most countries telecom incumbents operate within strict regulatory boundaries on how they can access and use customers' personally identifiable information, such as call logs, location and the like. Consequently, carriers have given a wide berth to services that could trigger legal liability.

Second, communications providers are keenly aware that technological innovation often outpaces consumers' ability to cope with it and understand all its privacy implications, leaving them feeling vulnerable and confused. Deep packet inspection (DPI) is a classic example. This technology offers such benefits as the personalisation of services, improved application performance and the ability to manage overall network traffic flows. However, it quickly became an industry "third rail" after many consumer advocacy groups highlighted potential abuses. Many consumers became quite concerned about its use, which curbed operators' plans to deploy DPI at scale.

"Managing personal data and digital identities is a natural evolution of the roles communications service providers have always played for their customers."

Interviewee,
"Rethinking Personal Data" project

This brings us to the third risk in the eyes of operators: losing consumer trust. Today, telecom operators enjoy a higher level of consumer trust than their Internet counterparts,[2] and thus have more to lose from experiments that are poorly received by the public. As the saying goes, trust is extremely hard to gain but very easy to lose. This dynamic will be increasingly important. The confidence individuals have in firms that manage personal data will need to be extraordinarily high. Individuals will be placing much of their lives in the hands of personal data stewards. Miscues on data integrity, transparency, security and accountability will have significant consequences.

Yet the gravest risk for the telecom sector may be inaction. Sitting back and delaying investment because of the ambiguity and complexity could result in missing this opportunity. Radically compressing cycle times in product development, time to market and regulatory approval will be critical areas of focus for telcos. The operational advantages Internet competitors hold in agility, innovation and customer behaviours will be extremely valuable.

The widespread use of live customer feedback to improve service offerings is another competitive advantage enjoyed by Internet firms. This "on-the-fly" improvement can be particularly

[2] Nokia Siemens Networks Privacy Survey 2009.

difficult for CSPs to embrace as they have built their core value proposition on “five nines” of reliability.

Internet firms, in contrast, are in constant beta. They are continually evolving their service offerings. This ability to test, learn and adapt in real time – and at global scale – is one of their strongest competitive differentiators. Failure to recognise this dynamic – and how quickly the window of opportunity could close for operators – could be a blind spot with material consequences.

Web 2.0 firms like Facebook and Google are already conducting trials of robust, Internet-scale identity-management systems. The real-time insights gained from millions of individuals who adopt these new offerings grow daily at a compound rate. As Albert Einstein supposedly once said, “The most powerful force in the universe is compound interest.” While he was referring to monetary growth, the same principle applies to the cumulative insights that Internet firms gain by continually learning from virtually every mouse click.

The inference is clear. The relative advantages carriers currently enjoy in this space could rapidly diminish. The next 1,000 days (roughly three years) will be critical for the telecommunications sector to leverage its authentication and identity-management capabilities to build a sustainable position in the personal data ecosystem.

A number of enablers have already slipped through the hands of carriers. Indexing (and by default search and advertising) has been ceded to Google. Directories and the social graph are now the domain of Facebook. Location is being subsumed by mobile app developers, OS providers and handset manufacturers. Without a sense of urgency and willingness to innovate collaboratively within the sector, authentication may also join the ranks of lost CSP opportunities.

Indeed, strategists from telecom operators and equipment providers concur that within the next two to three years, the ability of CSPs to build a strong position in securely identifying and authenticating users on the mobile platform may be lost (see Figure 1).[3]

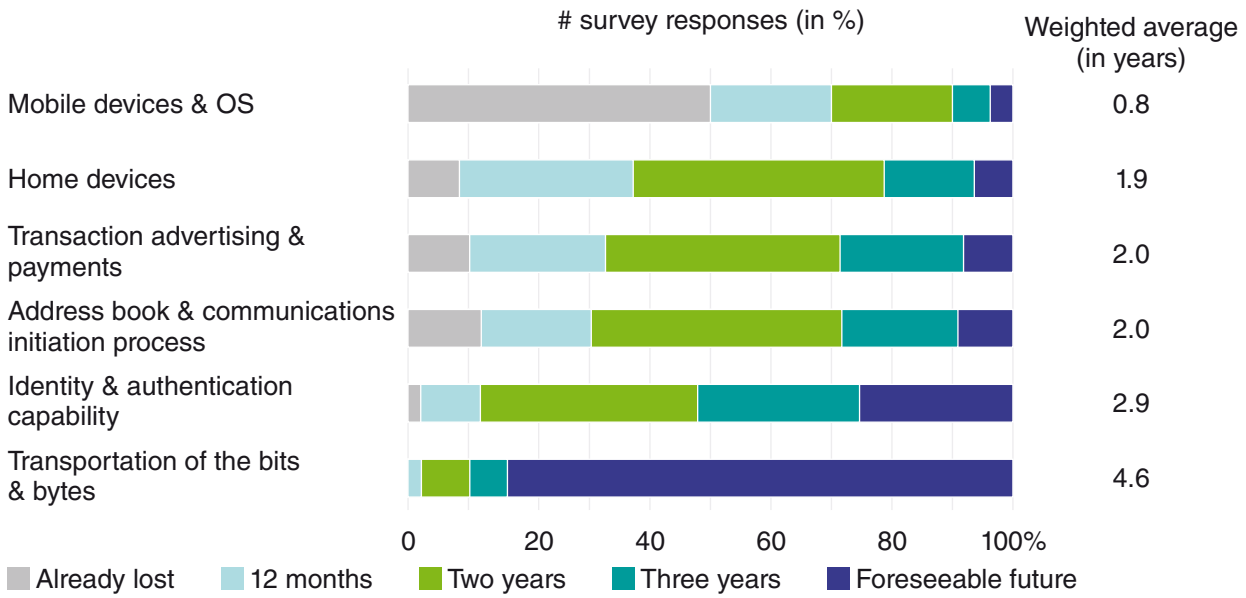
What options are open to operators? In its simplest form, the key opportunity is to build out what CSPs already do well. They should build on their robust security, identity and authentication capabilities developed primarily for enterprise customers (such as the capabilities that underlie a global, remote virtual private network or VPN offering) to develop services that are more consumer oriented.

This reorientation could take several forms:

- Offer “white label” capabilities for others to use;
- Provide wide access to these capabilities to third-party developers;
- Build proprietary services on top of these capabilities;
- Partner with other operators to gain scale and collectively reduce risk.

[3] STL Partners. Senior telecom executives survey (n=~200), November 2010.

Figure 1: Telecom executives survey: "How much time is left for telcos to retain or build a strong position versus internet players/other competitors?"[3]



Note: Weightings used to calculate weighted averages: "already lost" = zero years, "foreseeable future" = five years.

Whichever tack they take, CSPs will have to make trade-offs. For instance, if they partner, they must weigh time-to-market concerns against the benefits of both shared risk and greater scale. The last benefit includes the instant availability of a large addressable market, greater R&D resources and deeper marketing expertise.

More than these choices, the telecommunications sector will have to grapple with a personal data ecosystem that is highly complex, is moving very quickly and is filled with tremendous risk. But by framing this daunting challenge as a socioeconomic growth opportunity and organising around the needs of individuals, CSPs can greatly enhance their ability to create win-win-win solutions.

But despite the significant long-term growth potential, the over-riding feedback from project participants was to stay pragmatic and short-term-action oriented. In that light, five key areas of focus emerged for the telecommunications sector:

- Jointly innovate with other firms, inside and outside the telecom industry. Innovative concepts are emerging as an increasingly attractive means of creating Internet-scale, identity-management capabilities. One major factor is the Open Identity Trust Framework (OITF) model in the US. Telecom firms should invest with other firms in such trust framework models to foster overall market development.

- Partner within the industry and with other industry sectors to help shape regulatory policies on personal data. In many ways, the viability of emerging concepts depends on the outcomes of ongoing regulatory conversations about how digital personal data should be handled. Operators should collaborate closely with policy makers to help shape this outcome. In the US, developments surrounding the National Strategy for Trusted Identities in Cyberspace (NSTIC)[4] and the Federal Trade Commission's framework for "privacy by design"[5] should be closely monitored. In the EU, those in the communications sector should continue their dialog with the European Commission as it moves to revise the EU privacy directive and to synchronise legislation across its member states.[6] This is an area where telecom incumbents hold significant advantages over Internet and technology companies. They have deep experience in working with regulators to balance new business opportunities with cultural norms around consumer rights. Attitudes towards privacy are never a case of "one size fits all", and operators are usually more attuned to national and regional nuances in this area.

- Invest in streamlining patchwork, legacy network systems and internal organisational processes that restrict the ability of operators to quickly release new identity-management products and services. Firms that have already unified subscriber identities across Web, voice and cable products are well positioned to provide identity-management services outside the organisation.

- Support and develop open standards and the scaling of best practises. Recent telecommunications initiatives like the Wholesale Applications Community are important steps to develop and standardise the IT systems that allow the cross-silo sharing of personal data. But standards still face many challenges. The success of such initiatives is critical to foster the kind of third-party application innovation that will take advantage of operators' subscriber data and networks.

- Continue to support pilots focused on achieving Internet scale. Initiatives such as the Open Web Foundation could be very instrumental in aligning today's ad hoc standards and to enable the implementation of trust frameworks such as Mydex in the UK or the Open Identity Exchange in the US. Organisations like the IEEE have taken the lead in building on existing frameworks to define and promote open communication standards, particularly in areas critical to telecommunications firms.[7]

[4] NSTIC outlines a framework for trusted online identities and was developed in collaboration with key US government agencies, business leaders and privacy advocates.
[5] Federal Trade Commission. "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers" – preliminary FTC staff report. December 2010. http://www.ftc.gov/os/2010/12/101201privacyreport.pdf
[6] Ashford, Warwick. "Revised EU Privacy Laws to Demand Greater Transparency on the Web." ComputerWeekly.com. November 5, 2010. http://www.computerweekly.com/Articles/2010/11/05/243767/Revised-EU-privacy-laws-to-demand-greater-transparency-on-the.htm
[7] See Bain & Company's larger report for the World Economic Forum. "Personal Data: The Emergence of a New Asset Class." Page 35. January 2011.

Introduction

CSPs are under pressure to innovate

The telecommunication services industry has shown relatively steady growth during the last 10 years. Mobile access was the main impetus for profit growth, however, this growth has recently slowed to zero in developed markets and the rate of growth in emerging markets has declined.[8] Ahead, significant new challenges loom from the exploding growth in data.

The rate of increase in the amount of data generated by today's digital society is astounding. According to one estimate, by 2020 the global volume of digital data will increase more than 40-fold.[9] Beyond its sheer volume, data is becoming a new type of raw material that's on par with capital and labour.[10] As this data revolution era gains even more momentum, the impact on all aspects of society – business, science, government and entertainment – will be profound.

Given the fundamental shift in how value will be created in the digital economy, the telecom sector has little choice but to begin to explore ways to collaborate, innovate and differentiate in the use of personal data.

From a private sector perspective, the rapid growth of the largest Internet companies such as Google, Facebook and Twitter clearly shows the importance of collecting, aggregating, analysing and monetising personal data. These increasingly successful enterprises are built on the economics of personal data.

Personal data – a definition

For this report personal data is defined as data (and metadata) created by and about people, encompassing:

- Volunteered data – created and explicitly shared by individuals, e.g., social network profiles.
- Observed data – captured by recording the actions of individuals, e.g., location data when using cell phones.
- Inferred data – data about individuals based on analysis of volunteered or observed information, e.g., credit scores.

Source: World Economic Forum, June 2010.

Governments and public sector institutions are also transforming themselves to use data as a public utility. Many governments have successfully launched e-governance initiatives to improve the efficiency and effectiveness of communication among various public organisations – and with citizens.

But the deepest insights into the global personal data phenomenon come from understanding how individuals themselves are creating, sharing and using personal data. On an average day, users globally send around 47 billion (non-spam) emails[11] and submit more than 95 million "tweets" on Twitter.[12] Each month, users share about 30 billion pieces of content on Facebook.[13] The societal and

[8] Bain analysis of the mobile access profit pool, based on Capital IQ and Ovum data. 2010.
[9] IDC. "The Digital Universe Decade – Are You Ready?" May 2010.
[10] *The Economist.* "Data, Data Everywhere." February 25, 2010.
[11] The Radicati Group. "Email Statistics Report, 2009–2013." May 2009.
[12] "Twitter + Ping = Discovering More Music." Twitter blog, November 11, 2010.
[13] "Statistics." Facebook Press Room. January 11, 2011. http://www.facebook.com/press/info.php?statistics

economic impact of this "empowered individual" is just beginning to be felt.

No limits bound personal data's potential for creating vast new benefits for individuals, enterprises and societies alike. Imagine, for example, the decreased cost and increased quality of healthcare that a fully mobile electronic medical record could generate. Or picture the benefits from providing mobile financial services to the billions of people around the world who still have no access to the banking system. But unlocking this tremendous value depends on several contingencies. The underlying regulatory, business and technological issues are highly complex, interdependent and ever changing.

End user-centricity: a critical determinant in building the personal data ecosystem

"Rethinking Personal Data" project discussions have underscored the fundamental necessity of aligning the interests of all stakeholders: people, private firms and the public sector. Indeed, "win-win-win" outcomes will only come from a mutually supportive ecosystem. It must balance incentives, reduce collective inefficiencies and encourage innovation in a way that reduces collective risks.

This vision offers a future where:

- Individuals can have greater control over their personal data, digital identity and online privacy;
- Disparate silos of personal data held in corporations and government agencies will more easily be exchanged to increase utility and trust among people, companies and the public sector;
- The need by governments to maintain stability, security and individual rights will be met in a more flexible, holistic and adaptive manner.

In this vision, a person's data would be equivalent to their "money." It would reside in an account where it would be controlled, managed, exchanged and accounted for just like personal banking accounts today. These services could be exchanged with other institutions and individuals globally. As an essential requirement, the services would operate over a technical and legal infrastructure that is highly trusted. Maintaining confidence in the integrity, confidentiality, transparency and security of the entire system would require high levels of monitoring.

A key element for aligning stakeholder interests and realising the vision of the personal data ecosystem is the concept of end user-centricity. This holistic approach recognises that end users are vital and independent stakeholders in the co-creation of valuable services and experiences. End user-centricity represents a transformational opportunity. It seeks to integrate diverse types of personal data in a way that was never possible before. This can only be done by putting the end user at the centre of four key principles:

- Transparency: Individuals expect to know what data is being captured about them, the manner in which such data is captured or inferred, the uses it will be put to and the parties that have access to it;
- Trust: Individuals must have full confidence that the attributes of availability, reli-

ability, integrity and security are embraced in the applications, systems and providers that have access to their personal data;

- Control: This ensures that individuals will be able effectively to manage the extent to which their personal data is shared and at least own a "copy" of their data;

- Value: Individuals must understand the value created by the use of their data and the way in which they are compensated for using it.

Encouragingly, the mobile industry has taken initial steps in just this direction.[14] A suggested guideline of mobile privacy principles embraces the concept of Fair Information Practise Principles (FIPPs). It is an approach for educating corporations, policy makers and individuals on best practises for achieving privacy, security and the development of broad normalised information and identity service markets. The intent of this work is to address the complexity of managing privacy at global scale. Still in its early stages, some project participants suggested that it may need to expand beyond its current "storage and retention" paradigm to one that embraces the concept of enhancing data flows to increase the overall value of personal data.[15]

Communications providers are well positioned to participate in the personal data opportunity

Stakeholders of the "Rethinking Personal Data" project widely agreed that telecom operators are uniquely positioned to participate in creating value as they combine critical competences and assets.

- Personal data assets: Telecommunications providers already collect and manage an array of data about their consumers, ranging from volunteered data (such as individuals' addresses, sex or age) to observed data (such as phone usage times, website visits or current locations) and inferred data (such as crowd movement patterns, likelihood of visiting a specific website at a given time). Carriers could more effectively mine this data to build integrated "multi-screen" experiences, develop more targeted pricing plans and perhaps even partner with other companies to create innovative offerings. Among other ways would be to adopt such techniques as the airline-inspired "yield management" capabilities for matching interested customers with discounted seating at live events.

- The ability and infrastructure to process this data securely: Carriers have optimised their operating and business support systems to manage these different sets of data in a highly secure manner, particularly when authenticating network access, securing communication protocols and handling billing transactions. Many carriers have also already begun to work with such mobile OS providers as Google and Nokia to offer carrier billing for mobile applications. This could prove to be the platform for a broader foray into mobile commerce.

[14] GSMA. "Mobile Privacy Principles." January 27, 2011.
http://www.gsmworld.com/documents/GSMA_Privacy_Principles.pdf
[15] "Fair Information Practice Principles." Federal Trade Commission.
http://www.ftc.gov/reports/privacy3/fairinfo.shtm

- Access to the end user (across devices): Each user on the Internet or using a mobile phone has regular touch points with his or her communication service provider. Operators have made significant progress to ensure a 360-degree view of their customers, integrating all devices and channels. Solutions can be deployed quickly to many customers at immediate scale. The ability to provide authentication and digital rights management across multiple devices will be critical in providing compelling experiences that combine telephony, video and broadband offerings (such as TV Everywhere in the US).

- Trusted brands: Recent studies show that telecom companies are among the organisations that customers most trust to respect the privacy of their personal data.[16]

Operators will nevertheless face serious challenges. Future regulations, such as related net neutrality obligations or user data management, will have a large effect on the ability of communications providers to exploit personal data. Also, no one knows to what degree Internet companies are willing to cooperate with carriers in collaborating on solutions. Meantime, hampered by fragmented legacy systems and network innovation cycles that were measured in years, many CSPs struggle to bring new products and services to market as rapidly as Web firms do. Another concern: privacy issues, arising from more extensive use of personal data, might also undermine the trust individuals place in operators.

Despite these challenges, carriers such as NTT DOCOMO, Orange and AT&T are moving ahead in defining and deploying personal data services.

Below is a list of the principal growth opportunities for operators in the personal data ecosystem. It also illustrates which assets and competences are particularly relevant, as well as some illustrative offerings.

Three Principal Growth Opportunities within the Emerging Personal Data Ecosystem

Achieving stakeholder trust requires a set of legal and technical structures to govern interactions of participants within the ecosystem. The concept of trust frameworks is emerging as an attractive means for the personal data ecosystem to scale in a balanced manner. Trust frameworks consist of documented specifications selected by a particular group (a “trust community”). These govern the laws, contracts and policies undergirding the technologies selected to build the identity system. The specifications ensure the system reliability that is crucial for creating trust within the ecosystem.

Telecommunications firms could leverage their competencies and assets to participate in trust frameworks in various ways.

[16] Nokia Siemens Networks Privacy Survey 2009.

Operators as identity providers (IdPs)

The identity provider role is a natural extension of a carrier's core business. Identity providers issue, verify and maintain online credentials for a user. Participating websites ("relying parties") accept these credentials based on solid assurances that the IdP has proofed and validated the individual user in accordance with pre-determined specifications. This function ultimately enables all other categories of value creation within the personal data ecosystem.

Many operators have considerable experience providing identity-management services based on years of provisioning user access across multiple service offerings. Carriers routinely track users of their Internet or pay TV services. In the enterprise space, they may have even configured identity-management systems for small, medium and large businesses. Service providers also house vast amounts of verified customer data and have created customer service and billing capabilities that will be critical for identity-based services. Finally, with their large subscriber bases, service providers have the ability to deploy new service offerings at scale.

Potential business benefits

Attractive benefits could accrue from an identity provider role: first is the potential to generate new revenue streams by monetising the identity provider service. Relying parties would almost certainly be willing to pay for solutions that reduce losses associated with online fraud. Second, managing subscribers' online credentials while creating a more seamless experience should increase subscriber loyalty. For example, the ability to begin watching a live programme in your home, and then transition that experience to a portable device during a train commute, would both increase a consumer's loyalty and increase mobile data usage fees.

Some companies have already gained these benefits

Orange's Spanish subsidiary has found unique ways to monetise the data of consumers who opt in, while respecting individual privacy and providing a discount on monthly service charges. The firm accomplishes these benefits through its "Promo Tonos" offering. Using it, consumers can play commercial advertising jingles as ring-back tones to those who call them. Advertisers can target specific demographic segments, but no personal data is shared. Participants' discounts depend on the number of people who listened to the jingles. Orange receives remuneration from advertisers.

> *"Subscribers will be looking for help in using their personal data to simplify their lives and we believe that there is a strong willingness to pay for that help."*
>
> Interviewee, "Rethinking Personal Data" project

Movistar Argentina is another example. It recently partnered with Nokia Siemens Networks to provide an identity-management solution that gives customers a single sign-on capability. Movistar allows subscribers automatically to link their online identities on sites such as Flickr and Facebook, and it saves them from having to log in separately to each site.[17]

[17] Nokia Siemens Networks. "Movistar Argentina to Link Customers with Their Online Identities" (press release), 2009.

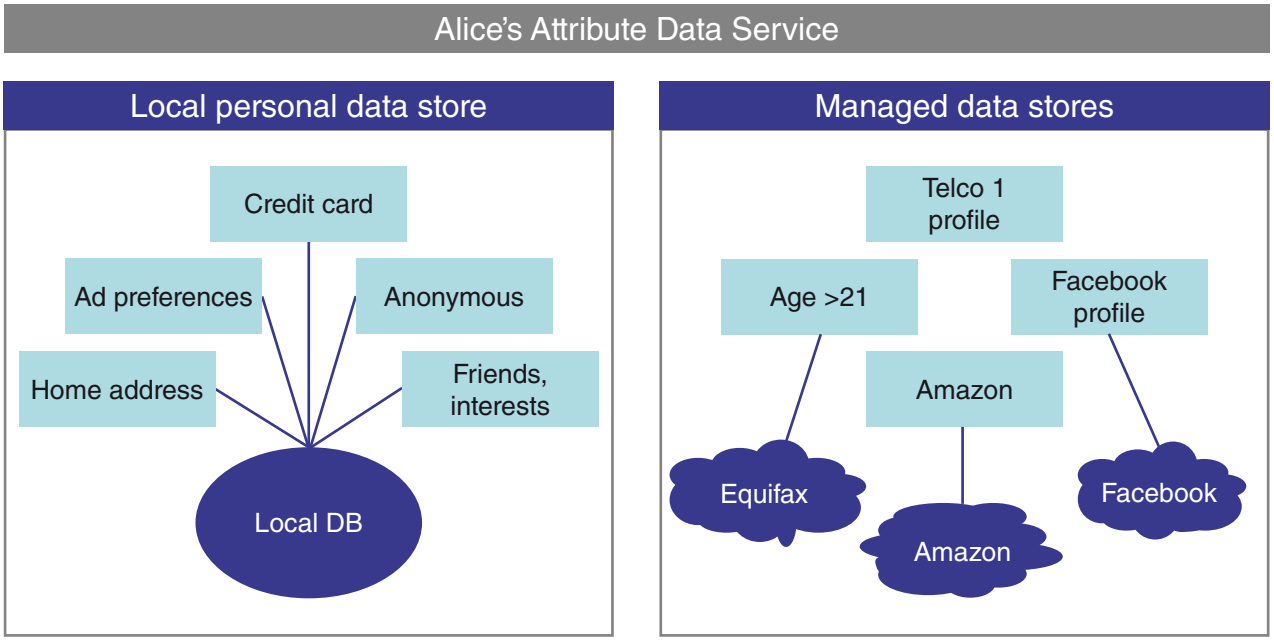
Operators as personal data service providers

Personal data services offer consumers a safe means to store, manage, share and gain benefit from their personal data. Such services consolidate users' digital identities, allowing them fully to control who, how and when it is accessed by third parties. The data stored in a "personal data store" can range from self-asserted attributes like an individual's preferences and interests to such managed and verified attributes as a person's age, credit score or affiliations supplied by external entities like Equifax or government agencies (see Figure 2).

Operators are well positioned to be personal data services providers to their subscriber base in more than a technical sense. As noted above, a 2009 study revealed that carriers are among the most trusted organisations by customers to respect the privacy of their personal data.[18] This will be another instance where telcos will be able to extend their billing and customer service capabilities.

While it may be a valuable service merely to store user's data, operators can do more for their subscribers by helping them make sense of and gain benefit from their data. Most subscribers would be willing to pay for such essential services. In fact, they already are.

Figure 2: Personal data services store end users' data and provide applications that enable them to manage, share and gain benefit from their personal data[19]



Source: The Eclipse Foundation

[18] Nokia Siemens Networks Privacy Survey 2009.
[19] Higgins Open Source Identity Framework.

AT&T has announced its intention to explore this very concept. As AT&T's customers connect using dissimilar devices, AT&T no longer has sole influence on its customers' experiences. The firm is thus investing in services to support customers across all access channels – in particular, helping them to manage their personal data. Indeed, AT&T developers are working on services that wrap individuals' personal data in a "protective layer." The idea is to give consumers greater control over how much data they share with third parties during commercial transactions. AT&T would function as a trusted agent, further deepening its customer relationships. As it explores these business opportunities, AT&T is searching for ways to scale such services and ensure the interoperability of emerging solutions. The firm regards common, open standards and the collaboration among solution providers – whether carriers or Internet firms – as crucial to unlocking this market's potential. For instance, AT&T is actively supporting Open Identity Exchange (OIX), an open market solution to provide digital identification-assurance services.

Potential business benefits

Another example is NTT DOCOMO's i-concier service, which is akin to a personal assistant in your phone. While not a complete data store, i-concier takes the subscriber's personal data – including location, preferences and the like – and combines these with data from other sources. This transforms the subscriber's cellular phone from a one-dimensional communication device to a lifestyle-support tool.[20] The Japanese mobile phone provider describes i-concier as an intelligent clearing house for collecting customer-selected information from unrelated services. These can range from weather, transportation and sports to coupons and other special offers. Within the first five months of its launch, NTT DOCOMO accumulated more than one million subscribers.

CSPs as third-party platform providers

An operator that has been successful as an identity provider and personal data services store can also operate as a platform for third-party entities that have developed personal data-based applications and services. The CSP's role would be to provide a user-controlled environment where subscribers can access a rich array of applications. These could be integrated with their cellular phones and personal data stores to provide advanced lifestyle support services.

CSPs operate one of the most complex infrastructures on earth. OSS/BSS[21] are optimised to handle a massive amount of data in a highly secure manner. User credentials are authenticated and network traffic data is analysed in near real time. Billing transactions are processed on a massive scale day and night. By giving third parties access to this infrastructure and related services (e.g., through open APIs[22]) CSPs could provide a leading-edge platform for external service providers to deliver innovative personal data services.

"One of the things I have been waiting for and not seen is the entrance in a truly major way of the CSPs into the health data space."

Interviewee, "Rethinking Personal Data" project

[20] NTT DOCOMO. "i-concier Service Heralds Age of Personalization." Mobile Quarterly. July 2009.
[21] OSS: operations support system; BSS: business support systems.
[22] API: application programming interface.

Potential business benefits

Subscribers will certainly be looking for help in using their data to simplify their lives and integrate their fragmented online experiences. One area of high potential is in health and wellness services. One can easily envision a set of services that centre on the consumer, his or her mobile handset and individual personal data. Such applications could, for instance, help people manage daily activity levels, diet and the ability to notify an individual's primary care provider if certain designated thresholds were passed.

Many Challenges and Open Questions Remain about Business Models

In the US and UK,[23] some pilots for personal data business models are under way. Companies in Argentina,[24] Spain[25] and Japan[26] are also forging ahead on similar services, even outside of the construct of a trust framework. Despite this progress, however, many open issues must be resolved.

Relying parties must buy into the benefits of a user-centric and controlled personal data ecosystem

End users obviously have clear benefits from greater control and ownership of their data. However, this effectively prevents companies from continuing freely to collect the rich data they traditionally use for customer relationship management purposes. Indeed, under some emerging business models, relying parties in a trust environment would have to start paying consumers to access their personal data stores. That begs the question of why a relying party would start paying for what was once free. Two significant reasons present themselves.

The first argument is to that no relying party knows more about the consumer than the consumer himself. The data in an individual's personal data store represents his or her complete digital identity. Companies today need to compare the value of mining that trove to sifting the bits and pieces existing on their servers today. In short, consolidated data is not only better quality data, it allows firms better to shape and customise their offers to consumers.

Second, the sheer cost of online fraud should be enough to make firms seriously consider participating in such a model. On

[23] Heath, William. "New Demos Book Includes the Long View on Personal Data." Mydex. May 5, 2010. http://mydex.org/2010/05/05/new-demos-book-includes-the-long-view-on-personal-data
[24] Nokia Siemens Networks. "Movistar Argentina and Nokia Siemens Networks Win Global Telecoms Business Award for Business Service Innovation" (press release). June 8, 2010. http://www.nokiasiemensnetworks.com/news-events/press-room/press-releases/movistar-argentina-and-nokia-siemens-networks-win-global-telec
[25] Orange. "'Orange Mobile Targeting Monitor' Launches in Europe, a New Intelligent Campaign-Planning Tool for Advertisers, Exclusively from Orange" (press release). October 6, 2010. http://www.orange.com/en_EN/press/press_releases/cp101006en.jsp
[26] NTT DOCOMO. "'i-concier' Service Heralds Age of Personalization." Mobility Quarterly. July 2009. http://www.nttdocomo.com/binary/press/mobility_doc_24.pdf

average, online fraud annually represented 1.2 per cent of a Web retailer's 2009 revenue.[27] The ability to stem at least some of that cost should be enticing to retailers.

Finding User-Centric Business Models That Work

Trust frameworks and personal data services require a user-centric business model. Achieving individual consumer buy-in requires attaining consumers' complete trust, constructed from the building blocks of personal privacy, protection, benefit sharing, control and transparency. None of personal data's vast potential will be realised unless user-centric business models are employed. But some question whether users really want the hassle of managing all that data. Innovative applications must allow users easily to maintain their data using intuitive, seamless and perhaps even automated tools.

Collaboration among operators and coordination to achieve required portability

Consumer buy-in for personal data services will also require enabling portability of the user's personal data, since users probably will not want their personal data "locked up" with any one CSP. The value proposition for consumers is greater if all carriers offer these services and consumers have complete freedom to move between CSPs. That suggests a high level of interoperability between carriers, which will require their collaboration and careful coordination. But will enough CSPs in each market be able to achieve this level of cooperation?

Competition for the user's identity

CSPs may very well be suited to play a central role in a user-centric digital universe. But they should realise that these roles need not be exclusively theirs.

"Transparency and education on how their personal data is being used are paramount to gaining end user trust."

Interviewee, "Rethinking Personal Data" project

In fact, a number of fiercely competitive Web 2.0 players are already working hard to establish themselves as the most trusted identity providers. Rushing ahead are Google, Equifax, PayPal and others. All offer identity-provider services in pilot roll-outs using the Open Identity Exchange (OIX), a trust framework provider in the US. Under this scheme, users can now log into an array of websites using their Gmail credentials. Other examples of new trust frameworks include Kantara's Identity Assurance Framework.

Google, Facebook, Microsoft, Equifax and a number of start-ups are also vying for the role of personal data services provider. Facebook, in particular, appears to have a head start with its volumes of data collected on more than 500 million users. But much of that data is self-asserted, which although an important source of data, cannot be the only one. Yet progress has been hampered as multiple privacy incidents have eroded end user trust.[28] So far, no single company has cornered the end user's digital identity market, but many are trying.

[27] "11th Annual Online Fraud Report." Cybersource, 2010.
[28] See, for example, Valentino-Devries, Jennifer. "What They Know About You." *Wall Street Journal.* July 31, 2010. http://online.wsj.com/article/SB10001424052748703999304575399041849931612.html

CSPs Must Act Now to Participate Meaningfully in the Personal Data Explosion

The explosion of personal data is both real and game-changing as it continues dramatically to redefine consumer's experiences both online and offline. But while no one can predict the exact nature of tomorrow's ecosystem, telecommunications companies can take some practical steps to position themselves to be significant participants. They fall under five categories:

1. Jointly innovate with other firms, inside and outside the telecom industry. Innovative concepts are emerging as an increasingly attractive means of gaining stakeholder trust and Internet-scale identity management; one example is the Open Identity Trust Framework (OITF) model in the US.

   Outside the US, companies like Movistar Argentina have developed their own identity-management solutions within circles of trusted relying parties. Carriers should collaboratively test and promote efforts like these to explore and develop their potential to provide Internet-scale, identity-management services to their subscriber base.

2. Partner within the industry and with other industry sectors to help shape regulatory policies on personal data. The viability of emerging concepts hinges almost entirely on the outcomes of ongoing regulatory conversations about how digital personal data must be handled. CSPs should collaborate to help shape this outcome. In the US, they should follow developments of National Strategy for Trusted Identities in Cyberspace (NSTIC)[29] and the privacy bill, and contribute to them. One way is to participate in the Federal Trade Commission's recent staff report on consumer privacy practises. In the EU, carriers should work closely with the European Commission's efforts to revise the EU privacy directive and to synchronise legislation across its member states.[30]

3. Invest in streamlining patchwork, legacy network systems and internal organisational processes that restrict the ability of operators to quickly release new identity-management products and services. Carriers that have already unified subscriber identity across Web, voice and cable offerings are well positioned to provide identity-management services broadly.

4. Support and develop open standards and the scaling of best practises. Such recent initiatives as the Wholesale Applications Community represent important steps forward. But standards still face many challenges. Success of initiatives like these is critical to foster third-party application innovation that can build off carriers' existing subscriber data and networks.

[29] See, for example, SecureID News. "National Strategy Delayed." November 18, 2010.
[30] A revised EU privacy directive is scheduled to go into effect in 2011, after a period of public consultation through the European Commission's website in January. Ashford, Warwick. "Revised EU Privacy Laws to Demand Greater Transparency on the Web." ComputerWeekly.com. November 5, 2010.

5. Continue to support pilots focused on achieving Internet scale. Initiatives such as the Open Web Foundation could be very instrumental in aligning today's ad hoc standards and to enable the implementation of trust frameworks such as Mydex in the UK or the Open Identity Exchange in the US. Organisations like the IEEE have taken the lead in building on existing frameworks to define and promote open communication standards, particularly in areas critical to telecommunications firms.[31]

Conclusion

Personal data will radically transform customer experiences, both online and offline. Telecommunications carriers have two choices: they can let the personal data trend pass them by or they can pragmatically hone their core capabilities to participate actively in the opportunities that have already begun to unfold.

When making this decision, CSPs should consider that they are extremely well positioned to benefit from the explosion of personal data and to build viable business models around it. Carriers still have built-in advantages against other firms, such as their ability for massive-scale identification and authentication.

However, these advantages have already started to diminish. Competitors are very likely to catch up within the next few years. If CSPs want to engage in the personal data opportunity, the time to do so is now.

No single operator can unlock the personal data market alone. Telecommunications firms need to work together and across industries. Carriers can take pragmatic steps now and we recommend focussing collaborative actions on the five areas above.

Whatever choices CSPs make over the next critical 1,000 days, one thing is certain: The personal data ecosystem will have a transformational impact on consumers and firms – with or without carriers' involvement.

[31] See Bain & Company's larger report for the World Economic Forum. "Personal Data: The Emergence of a New Asset Class." Page 35. January 2011.

COMMITTED TO
IMPROVING THE STATE
OF THE WORLD

The World Economic Forum is an independent international organisation committed to improving the state of the world by engaging business, political, academic and other leaders of society to shape global, regional and industry agendas.

Incorporated as a foundation in 1971, and based in Geneva, Switzerland, the World Economic Forum is impartial and not-for-profit; it is tied to no political, partisan or national interests.

World Economic Forum
91- 93 route de la Capite
CH – 1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744

email: contact@weforum.org
www.weforum.org