Reflections on the Use of Personal Data and the New Legal Framework for Data Security

Strategic Technology Forum
March 2011
Reflections on the use of personal data and the New Legal Framework For Data Security

“Personal data is the new oil of the Internet and the new currency of the digital world.”
Meglena Kuneva, European Consumer Commissioner, March 2009

As we move into 2011, the field of data security and privacy is developing into a fascinating mix of policy, legislation and technology, and has the potential to develop in to a new marketplace.

The combined effect of innovation across mobile internet, smart-phone and tablet devices, big-data science, e-commerce, digital advertising and context-aware computing has brought the long standing issue of personal data security to a head.

Adding to the drama is the realisation that personal data is an extremely valuable resource. Indeed, personal data has been transformed, as if by the alchemist's touch, into gold: or at least, according to the WEF, a "new asset class" (see World Economic Forum report: "Personal Data: The Emergence of a New Asset Class")¹.

For some groups of consumers, the problem has switched from protecting their personal data to generating economic value from it. Interestingly, this market-driven approach may well turn out to be a viable protection mechanism.

The blossoming of start-ups in this area and the emerging market in privacy and “data property rights” over the last 12 months after a 10 year hiatus in privacy and security is covered in an interesting article in the Wall Street Journal on the 28th February ². The WSJ has also run a series of investigative articles under the banner “What they know”³.

In 2010, privacy concerns with both Facebook and Google were front-page news. (Facebook’s controversial ‘Beacon’, an attempt at ‘word of mouth’ advertising was shut down in 2009.)

Even for mundane devices such as electricity meters: witness the recent privacy concerns around Smart Grid technology. While the benefits of smart-grid technology for improved management and reliability of energy and resources are self-evident, there are unanswered questions about the protection of the data collected and what it can be used for. The real-time measurement of energy consumption in our homes enables detailed insights into our personal worlds.

As more and more devices and parts of our personal lives get connected to the net, privacy becomes more complicated and the consumer is losing more control of personal data. And it is precisely in response to consumer data privacy concerns that the regulators have been hard at work.

Last month the US Federal Trade Commission published a draft report – “A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers”⁴ presenting a framework to “balance the privacy interests of consumers with innovation that relies on consumer information to develop beneficial new products and services”. Notably, the FTC observes that self-regulation has

²http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html
⁴Available at http://www.ftc.gov/opa/2010/12/privacyreport.shtm
been too slow, and recommends a “privacy by design” approach as well as a “do not track” capability.

Meanwhile in January this year the US Commerce Secretary announced3 the formation of a program office within the Department of Commerce to “coordinate federal activities needed to implement the National Strategy for Trusted Identities in Cyberspace (NSTIC)”. This is an Obama administration initiative aimed at “establishing identity solutions and privacy-enhancing technologies that will make the online environment more secure and convenient for consumers.”

In Europe the EU is proposing new legislation with the intent of strengthen individuals’ rights, including the right to be “forgotten online”. ("A comprehensive approach on personal data protection in the European Union")⁶. How these developments play out, and over what time frame, remains to be seen.

What we can be sure about is that privacy and personal data security has become a major compliance issue. However, compliance is not enough. The protection and use of personal data is heavily nuanced by the unique concerns and preferences of individual consumers.

Consumers have increasingly strong views on how and when they communicate with the organisations they do business with, the kinds of communications they which to receive, and through which communication channels.

It is becoming increasingly critical for organizations to be able to manage these individual customer preferences, including the use of personal data, and to use these to manage - in real-time- the personalization and delivery of communications across different channels and devices, whether a printed letter or a marketing offer pushed to a customer’s facebook page on her smartphone.

As in all relationships, privacy has many nuances. Organisations will not only have to ensure that they comply with legislation governing privacy: in addition they must have the ability to communicate with each customer according to their individual preferences and needs.

The legal framework, comprising government policy, legislation, regulatory guidance, enforcement as well as standards for best practice, provides a foundation. But organisations will need to embrace the principle of “security by design” and build security awareness into business processes and structures.

Organisations, especially those in regulated sectors such as banking, insurance and healthcare or in the public sector, need to manage the use of personal data to meet not only the requirements of data protection, but also as part of a proactive customer communications strategy that demonstrates the responsible use of personal data. Consumers are increasingly aware of the value of their personal data, the uses and derivative uses of that data, and its vulnerability.

In order to achieve these goals, organizations will need the following capabilities:

- The ability to manage the use of personal data in customer communications across all communication channels (regardless of the device).
- All content, metadata and business rules should be held in a central location and shared, making regulatory-required changes simpler and more efficient.

---


• Single source of content – a single source “write once, publish many” model - keeps to a minimum the number of documents containing critical compliance content and personal data elements.
• This means no silos – departmental silos are the source of much of the fragmentation and duplication of data and content that leads to lack of control and data leakage.
• Work-flow approval - compliance and legal departments should be fully integrated into the approval cycle ensuring documents and the personal data they use comply with the relevant standards.
• Integration with business rules and application logic to ensure that the use of personal data and content is consistent with enterprise/customer data and rules, and reduces scope for error.
• Granular control and authenticated role-based access to data and document templates and rules that use personal data.
• Increased accuracy and timeliness of information shared across organization – and a corresponding decrease in the quantity of bad data (inaccurate, out-of-date information) percolating through the enterprise and out to the customers
• Enable line of business users to work directly with the application of personal data to business communications.
• Visibility into the impact of changes, illustrate what data is affected by proposed changes and what’s required to affect a regulatory modification.
• Audit trails - full auditing means that output documents and communications can be traced back through the authoring, approval and production process.

Conclusion

Despite the strong foundation provided by the framework of policy, legislation, best practice, guidance and enforcement, organisations face a more complex challenge for personal data security: customers who have a range of different needs and requirements for the use of their personal data and who understand the value of that data. In order to prosper, organisations will need to be able to engage with each customer on a unique basis, taking into account their individual preferences for communication and use of their personal data.