Sören Preibusch

University of Cambridge
Computer Laboratory

15 JJ Thomson Avenue
Cambridge CB3 0FD

Soeren.Preibusch@cl.cam.ac.uk

2010-06-07

Comments regarding the Notice of Inquiry on
Information Privacy and Innovation in the Internet Economy

Unaddressed privacy concerns lead to welfare loss

Privacy has become a decisive factor for the success of online transactions. Whilst more recently, privacy negligence at global social networks has sparked protest form consumer associations, governments, and interested individuals, electronic commerce has been exposed to the negative consequences of careless data processing for a longer time.

According to a 2009 PayPal-commissioned study, protecting their privacy and the related protection from fraud and ID theft are online consumers' two biggest concerns when shopping online. Earlier surveys indicate that two thirds of offline-only shoppers did not purchase online because of privacy concerns; around one third of online shoppers would buy more if they were not worried about privacy/security issues; more than a quarter of shoppers had abandoned online shopping carts because of privacy reasons. My own research indicates that two thirds of online shoppers intend to cancel a transaction if prompted for personal information they are unwilling to provide. The majority of them choose to switch to an alternative, competing vendor, and approximately 30% provide false information, leaving the online retailer with untapped sales potential and latent defects in data records.

As consumers refrain from shopping online because of privacy concerns, the loss in realised trade implies a loss in social welfare.

Naive anonymity is not the answer

Simply reducing data collection does not provide a viable route to increase consumers' propensity to shop online.

Anonymous usage of online services is often undesirable as it forbids a persistent account with convenience features such as a transaction history or reuse of once-entered information.

Anonymity also precludes the ability to personalise offerings, a basis for recommendations individually tailored to one's needs and interests. As identity information is used in addition to the behavioural and transactional profile, socialising features amongst consumers are unlocked. Whilst there is a clear business perspective in such marketing endeavours, consumers actually value the convenience and quality of personalised services.

As we acknowledge that anonymity is not the aim, we also realise that security features such as data encryption alone are insufficient, despite being an important building block of privacy-enhancing technologies.

Information privacy is achieved through individual control

Privacy is an individual's ability to decide for herself who should have what information about her and also the individual's ability to effectively limit how this information is used, for which primary and secondary purposes, and with whom it is potentially shared.

Privacy reaches beyond the data item itself. Privacy requirements put personal information in context, notably through purpose-binding. For instance, whilst a consumer may decide to reveal her email address to an online shop, she may want to restrict how her email address is being used: order confirmations are acceptable, but a weekly newsletter is unsolicited. Currently, Web interfaces seldom offer even such basic methods for users to exercise choice and control.

The Notice of Inquiry uses the term "use-based rules" to describe user-driven regulation of purposes for which personal information may be employed. I argue that effective choice in privacy-related decision-making does and should genuinely encompass users' ability frame their personal details.

In some continental European legislations (e.g. Germany), companies are forbidden to tie customers' acceptance of the terms and conditions to consenting the privacy policy. Pragmatically, this leads to two checkboxes on Web forms; more philosophically, it implements the distinction between primary and secondary purposes of data usage for the same set of data items.

Heterogeneity in privacy preferences

The why and how of one's control over the own personal information very much depends on privacy preferences albeit the data subject's routine inability to verbalise these preferences. My own research into *privacy types* shows the difficulty in structuring a population of consumers into groups that exhibit similar concerns about revealing personal information. Consumers have fragmented preferences with regard to providing personal information online, let alone the moderating effects of trust and previous interactions at the individual level. Even fine-grained clustering achieves poor coverage of the entire online population.

This heterogeneity implies that any attempt to approach consumers with an inflexible, take-it-or-leave-it privacy policy—as it is current corporate and regulatory practice—will leave most of consumers unsatisfied.

Detrimental inflexibility in current privacy practices

Consumers' diversity in privacy preferences and their individual valuations of service quality levels unlocked by additional, voluntarily provided data, find little response in current data collection practices on the Web.

Today, the parameters of informational self-determination are often laid out in privacy policies, but it is hard to find user participation in these policies when flexibility or feedback channels are absent. As frustrated and disappointed customers cancel online purchases, or avoid online interaction because of privacy worries, companies are unable to learn which parts of their static privacy policy lead to rejection at the individual level and how the dependent functional service properties are valued. Consequently, the existing channels of the Web for interaction and transaction do not tap into their full potential.

Subjective choice and objective guide

The Notice of Inquiry contrasts "satisfying subjective consumer expectations" with "enact[ing] objective privacy principles" as design goals for regulation. These goals are not mutually exclusive, all the same. Subjective satisfaction is achieved as consumers make individual choices. To the extent these choices are guided by appropriate risk assessment, i.e. privacy decisions really reflect informed consent, they translate an objective principle. Regulation could encourage effective support tools, increase the salience of privacy risks, make implicit data collection explicit or mandate privacy-friendly default settings.

Privacy Negotiations

The relationship between privacy and personalisation has been labelled as a trade-off; however, this term ignores the rewarding ability to also tailor data protection to the individual customer.

In *privacy negotiations*, consumers and service providers establish, maintain, and refine privacy policies as individualised agreements through the ongoing choice amongst service alternatives.

Negotiable privacy policies put an end to the paradigms of take-it-or-leave-it and one-size-fits-all. Privacy policies become a matter of personalisation themselves. Privacy negotiations provide customers with the ability to choose the level of data protection they deem appropriate and desirable at that very moment. This principle of choice, which can happen implicitly as services are consumed online, is advocated in most culturally motivated data protection principles, such as the Fair Information Practice Principles.

By breaking down the opt-in process to single data items or other privacy dimensions such as secondary purposes, the retention period, and sharing with third-parties, privacy negotiations also follow the spirit of the European Privacy Directive. Disagreement on a single aspect of the privacy policy no longer implies that the customer is forced into a data collection scheme against her will or to cancel the transaction; instead, the user may singularly choose not to provide a data item.

Offering rewards for specific data items expands the negotiation space and thereby makes reaching an agreement in privacy policy negotiations with higher levels of data disclosure more likely. In *incentivised privacy negotiations*, the transaction partners may additionally bundle the personal information collection and processing schemes with monetary or non-monetary rewards. Live examples include discount codes attached to a newsletter opt-in.

Privacy negotiations are a win-win for consumers and corporations

Privacy negotiations allow consumers to effectively find, for themselves, a balance between their privacy concerns and their appreciation for online services, for which voluntary data disclosure potentially unlocks more advanced features. In embracing the diversity in privacy preferences, fewer consumers are deterred by subjectively worrying privacy practices. Companies may offer incentives to stimulate voluntary data revelation as mandatory collection is phased out.

The exchange of personal data items for rewards does not conflict with the nature of privacy as a fundamental human right which excludes it from being traded. Privacy negotiations do not contravene the human right to informational self-determination. Consumers are not rewarded for renouncing their privacy, but agree on a price for personal information, which is an economic good. As a privacy-enhancing technology, incentivised privacy policy negotiations lift this price above null compensation.

Companies, in turn, may realise that consumer-friendly privacy practices attract new socio-demographic milieus. My research provides evidence that a company charging slightly higher prices, but collecting less personal details may sell commodity products at an average unit price of 80% above its competitor's price, effectively turning privacy into a competitive advantage.

Mechanised enforcement generates trust

As a result of privacy negotiations, combinations of data items agglomerate to amorphous data records. Even similarly filled data records may be governed by different privacy policies. This poses new challenges for the back-end data processing algorithms. Consequently, stronger assurance must be given that not only some, company-determined static policy is respected, but that every user's own privacy configuration is diligently adhered to.

The Notice of Inquiry asks how "privacy-related technologies and business processes [could] enhance consumer trust in Internet commerce." Privacy seals are the most salient advertising of

careful processing of personal information; if vouched for externally, certification often involves scrutiny of the companies' data processes. However, the degree of formality of such assessment remains low with code inspection being rare and mechanised analysis even rarer. Therefore, seals are only as reliable as the laborious manual inspection. Their costs also make privacy checks less frequent than changes to the functionality of the Web site, resulting in potential divergence between the certified state and the actual state. Further empirical and theoretical research is needed to bridge between empirical research into the economics of privacy and formal *privacy calculus*.