



Comments before the Federal Trade Commission re:

Information Injury Workshop and P175413

Introduction

With offices in DC and Brussels, the Developers Alliance is the world's leading advocate for software developers and the companies invested in their success. Alliance members include industry leaders in consumer, enterprise, industrial, and emerging software development, and a global network of more than 70,000 developers. We welcome this opportunity to engage with thought leaders and the public on digital privacy.

As the Commission's background document recognizes, "Information flows drive the economy." The movement, analysis and reconfiguration of billions of small data points is yielding tremendous insights and driving innovations in medicine, manufacturing, science and our social sphere. Without the free-flow of data, the digital economy withers, and social benefits are lost. Consumers already benefit tremendously from this new economic model, and it is critical that policy makers work to preserve these benefits at home and abroad.

It is also critical to note that the digital economy is a large ecosystem supporting companies large and small. Smaller firms seldom have the resources to staff legal departments or manage bureaucratic churn, so clarity, simplicity, and ease of implementation should be of paramount concern where policy makers seek to intervene.

The importance of data to the Alliance's membership is inseparable from their focus and unwavering desire to maintain consumer trust. From a business perspective, developers have a vested interest in ensuring their customers' expectations for privacy are met. In fact, developers work particularly hard to earn their customers' trust and have been among the best practitioners of data's golden rule: treat customer data in the same manner you would treat your own. Trust is a core concern for our members for a simple reason; consumers will not use services that they do not trust. Security, transparency, and data stewardship have become fundamental to business success in the digital economy, and our developer members are actively engaged in promoting best practices in these areas.

Finally, the Commission's outline assumes that managing the "trade-offs" between privacy and the benefits of the digital economy is a key driver for the ecosystem. We would point out that in many cases the benefits of the digital economy are the direct result of a consumer's own balancing of service value and information privacy, a very personal and highly varied decision process that in turn shapes many developer decisions. It is our hope that the evolving discussion around information injury will maintain a focus on identifiable and actual harms in the context of actual consumer behavior, rather than devolve into hypothetical harms and prophylactic measures driven by theories that are inconsistent with how consumers actually

act. As such, the FTC should focus its efforts on identifying clear, measurable and actionable harms that actually need to, and can be, remedied by the Commission.

Context: the Tools

In part, the complexity of the privacy discussion is due to the evolving nature of the internet and the economy it supports. Innovations in information security, internet architecture and governance, and emerging business models impact what is possible when discussing information injury mitigation. It is therefore important to understand the tools available to the ecosystem.

Encryption technology has made significant strides in recent years, such that it is now both possible and practical to secure personal data end-to-end across the ecosystem. Mass data breaches of strongly encrypted data pose a significantly smaller risk than data in the clear. Newer tools such as block chain can make fraud detection easier and promote trust between contracting parties. Cloud services provide decentralized and hardened storage and protected processing while limiting the duplication of data stores that drive vulnerability. Supporting systems such as multi-factor authentication now help consumers to protect their own data and make them a part of the security infrastructure. Taken together, there have been significant developer-driven technical innovations focused squarely on reducing information injury and safeguarding consumers and businesses alike – all without regulatory pressure.

A Framework for Privacy based on Trust Relationships

Unfortunately, too frequently data is associated with fear and danger instead of innovation and advancement. Data privacy and data breach are the focus of too many bad-news headlines and too many legislative and regulatory proposals. Far too many policymakers believe that data collection is a predicate to offensive behavior, rather than the bedrock of innovation and opportunity.

Consumers view their digital privacy in context, and this is a personal and varied calculus that is difficult to generalize. It is clear that consumers see tremendous value in sharing their data to enable the innovative services developers are building. In order to obtain a view of traffic congestion, consumers share their location and speed, knowing that if others do the same that all will gain from the insights. Or another example, providing a digital agent with enough information and context to act on your behalf, thus mimicking trust relationships in the off-line world. Or providing expertise as part of an aggregate decision making mechanism, by sharing experiences and tapping into the collective wisdom of large groups. In all these cases, there is an underlying trust relationship between the consumers involved as well as the service itself.

Trust breaks down in the face of outright breach, but also in unexpected or unanticipated behavior by a trusted party that causes harm to users. In the real world, many of the norms

that guide us are unwritten but implicit in everyday interactions and socially reinforced. The internet presents challenges in that many consumers are strangers to each other and may have differing social norms. How we map real-world trust mechanisms to online interactions is a difficult question with the potential to significantly impact the privacy debate. We encourage workshop participants to explore these areas as part of a comprehensive overview of the issue.

How Digital Businesses balance Value and Privacy

Business asks for data for different purposes: to enable a personal service, to enable a crowd service, for your security, to trade with others or to directly monetize to subsidize a service, to drive innovation, or because they are mandated to by government. Access to data is integral to small business, local business, local economies, and our global economy. The harms resulting from data breaches and data misuse must be addressed, but can be addressed narrowly – without unduly impacting companies’ opportunity to collect, aggregate, analyze and utilize data.

While it is common to talk about the “value” of data measured in terms of revenue generation, the greatest value is actually in the “utility” of data to drive innovation or service improvement, create consumer value, reduce risk, address security concerns, or meet regulatory obligations. The true value of data is ultimately measured in terms of business success or failure.

How Consumers Value Privacy

The fact that everyone – business owner, developer, or consumer – are also consumers in our own right is a key insight in understanding privacy in context. We join frequent flyer clubs, we fill out the census form, and we apply for loans and share our credit history. We all share the same feelings about privacy, varying by degrees not absolutes, and we adapt our behavior based on whom we trust and what we value. Developers are keenly aware of this dynamic, particularly since their goal is to produce a product that serves a need and that people value. In a nutshell, data is a tool not a goal, and trust is fundamental to a developer’s success.

What complicates things is that consumer’s actions and behaviors do not always align with how they articulate their position on privacy. Consumers want privacy, but are willing to provide the information needed to enable a service they value, or use a service subsidized through advertising. What’s clear is that consumer’s want to understand the relationship between the information they supply and the service they get. They want transparency so that they can make their own value decision. Transparency breeds trust. They then want to make their own personal decision on what they share and what they withhold.

This consumer-to-service relationship is complicated because the underlying nature of data is complicated, and because individuals operate within a community. In some cases, the state

may over-ride personal choice for social good. This creates challenges for developers who own the consumer trust relationship, and thus policy makers must be careful not to make industry an agency of their own purpose. In many cases, it is the complexity of what is included in “data” that creates the difficulty. Location data, for example, is a broad category: do we mean transient location, or a location history, or a location forecast? Does the service require location data in order to function, or to function better, or to benefit one consumer or many? An agreed taxonomy of the data space could help support a robust discussion.

Finally, forces external to the service-consumer relationship add another layer of complexity, as in the case of government surveillance or criminal behavior. Questions surrounding the degree of protection that a service can or should provide from unauthorized access are important. Even more important are regulatory restrictions that can actually limit developer’s ability to protect their customer’s data. Workshop participants should also spend time looking at existing rules and regulations that unhelpfully prevent data stewardship and security.

Conclusion

“Information flows drive the economy.” The benefits are so numerous that concepts like “balancing” and “tradeoffs” seem somehow inadequate to frame this important discussion. The Developers Alliance would encourage participants in this discussion to simply focus on how best to reduce the likelihood and impact of potential harms, and leave the benefits as a given.

For developers, there is no debate about the need for this conversation, as consumer trust is the bedrock upon which their success rests. The social, moral, and fiscal reinforcement mechanisms are already in place.

We believe that the technology that has the greatest near-term potential in reducing information injury is data security. Strong encryption is the universally accepted answer to reducing information injury by securing data from unauthorized access. Strong encryption deters criminal behavior by raising the cost to access useful information while simultaneously reducing the rewards of data theft. Strong encryption is relatively inexpensive to implement, well understood, effective, and academically proven. Removing impediments to security must be a key priority.

With security addressed, the trust relationship between digital services and consumers becomes much more of a personal dialogue about the use of one’s data. Its fundamental underpinning is transparency. Our focus should be on developing a language that captures the context-rich decisions that consumers already make in their daily lives, and adapting this to their digital interactions.

We look forward to an enriching discussion under the Commission’s guidance, and on behalf of our members welcome the opportunity to contribute to this important topic.

Bruce Gustafson
President & CEO
Developers Alliance
Washington, DC