Privacy and Value Co-creation for IT-enabled Service Systems: Cui Bono?

Ellen Chan  
Portland State University  
ellenpchan@gmail.com

Robert R. Harmon  
Portland State University  
harmonr@pdx.edu

Haluk Demirkan  
Arizona State University  
haluk.demirkan@asu.edu

Abstract

Almost all IT enabled service systems such as Google, Facebook, Apple, Microsoft, Skype are facing criticisms on their use of customer data and their failure to protect customer privacy. These service companies rely on customers to participate actively in the co-creation of value by providing personal information, data and preferences. Such important resources and assets, if mishandled by companies, can cause harm to customers. Misuse and poor privacy protection for customer information can create ethical, legal, and business consequences, diminish trust and inhibit relationship building between customers and service providers, and affect future value co-creation. This paper identifies the different facets of privacy, explores the intersection of privacy and co-creation of value, and offers suggestions for future research regarding how businesses and customers can benefit from the service while ensuring privacy is protected.

1. Introduction

In 1999, Sun Microsystems CEO Scott McNealy famously provided a prophetic assessment of online privacy: “You have zero privacy anyway. Get over it [57].” A decade later, Amazon, Apple, AT&T, Facebook, Google, Microsoft, Skysc, Sony, Verizon, and many others have fulfilled the prophesy as they experienced severe breaches of their online systems that have compromised private customer data on an unprecedented scale [1][4][13][35][39][60][63]. All of these organizations’ IT service-driven business models depend on information that results from value co-creation relationships with their customers and business partners. But, few customers fully realize that they are engaging in an information market where the value that is willingly co-created may be asymmetrically in favor of the online service firms [43]. The multiple breaches of confidential personal data, it’s misuse and leaks, and abuse of information collected by internet service and mobile computing providers cause people to wonder if privacy is indeed “non-existent [15].”

Interestingly, although upset about compromised identities and lost trust in their service providers, customers continue to embrace, rather than abandon, the sharing of information with Internet service providers [49]. Service firms continue to extract business value from and capitalize on sharing consumers’ personal information, mostly for targeted advertising and other marketing activities [64]. This situation raises the privacy concern, and ultimately, trust in the co-creation of value relationship between service providers and their customers.

The purpose of the article is to explore the potential impact of information-based service delivery on consumer privacy with respect to value co-creation within the context of the service-dominant logic [66], provide a framework (the four dimensions of privacy), explore foundational privacy issues and articulate an agenda for future research. We believe this is one of the first articles to review privacy related issues in context for today’s advanced IT enabled service delivery mechanisms.

The article is organized as follows. First, we provide an overview of consumer privacy and its various elements. Second we identify and explore personal privacy issues that are endemic to co-creation of value for online service providers. Finally, we offer insights for the development of future research.

2. Privacy and Information Markets

Warren and Brandeis in their 1890 Harvard Law Review article defined the right to privacy as “right to be let alone [69].” They pointed out that the new technologies of the time; newspapers, telegraph, and photographs, represented potential threats to personal privacy. Since then, much of the literature on personal privacy has been synthesized predominantly from the legal perspective, especially for information-related issues [54]. From a service delivery point of view, it is important for businesses and customers to fully understand the dimensions of privacy and the factors that contribute to the erosion of personal privacy.

Recently, services enabled by networked smart systems, are considered by firms such as IBM, Oracle, Microsoft, Google, Apple, and Cisco as “the next big thing [33][53].” IT-enabled online services create an information market with data as “a new form of currency [3].” Web 2.0 principles emphasize customer engagement, user participation, openness, collaboration, and network effects that can enable the co-creation of value. Software, sensors, infrastructure, computing devices, systems and networks are connected and converged for the delivery of innovative online services. One example is the popular use of smart phone applications that provide location-based
information and other mobile services [53]. Another is the emergence of social networking sites such as Facebook that enable users connect with others, nurture relationships and generate social capital [19]. The information services are convenient, time-saving, economical, fun, and immediate [2], making them appealing to consumers.

On the other hand, this “explosion of bits” has caused customers to lose, abandon, and generally fail to protect their privacy. They unknowingly leave “footprints and fingerprints” in the digital world by the consumption of Internet technology. User data sporadically left in the cyberworld as digitized bits can become permanent, un-erasable records [54][55]. This information can be readily aggregated to form a profile of a person’s behavior, lifestyle, personality, and reputation; whether complete, fair, or unauthorized [54]. Sensitive financial information and health records can be made public either on purpose or by mistake [55]. The possibility to track or expose one’s whereabouts can potentially cause personal safety concerns [5]. Private information can now become public instantaneously and be shared in different channels worldwide.

New mobile technologies such as Wi-Fi, 3G and 4G networks; tablets, smart phones, and mobile apps; have encouraged behavioral change by customers. Coincided as “Generation Google,” young people rely on the Internet to disseminate their own information and ideas and stay in touch with the world [2]. Obviously, some users are not concerned about privacy. However, a 2010 study led by the Berkeley Center for Law & Technology indicates that young adults are sensitive about online privacy and have favorable attitudes towards the adoption of more stringent policies. This finding refutes claims that they are ignorant or casual in terms of online privacy. However, young adults’ mistakenly assume that their privacy is being fully protected under the existing legal environment [9][30].

2.1. Defining Privacy

Online information technology services have raised concerns about privacy for some time [23]. Warren and Brandeis’ “right to be let alone” definition was raised under the technology boom in the late 1800s [69]. More than 100 years later technology-driven privacy concerns are an increasingly important topic for service users, businesses, academia, government, and society.

<table>
<thead>
<tr>
<th>Concept</th>
<th>Year</th>
<th>Author</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>The right to be let alone</td>
<td>1890</td>
<td>Warren and Brandeis [69]</td>
<td>“Right to be let alone”</td>
</tr>
<tr>
<td></td>
<td>1958</td>
<td>Douglas [62]</td>
<td>“Right of privacy includes the privilege of an individual to plan his own affairs”</td>
</tr>
<tr>
<td>Limited access to self</td>
<td>1880</td>
<td>Godkin [26]</td>
<td>“The right of every man to keep his affairs to himself, and to decide for himself to what extent they shall be the subject of public observation and discussion”</td>
</tr>
<tr>
<td></td>
<td>1970</td>
<td>Breckenridge [14]</td>
<td>“The rightful claim of the individual to determine the extent to which he wishes to share of himself with others”</td>
</tr>
<tr>
<td></td>
<td>1983</td>
<td>Bok [11]</td>
<td>“The condition of being protected from unwanted access by others—either physical access, personal information, or attention”</td>
</tr>
<tr>
<td></td>
<td>1992</td>
<td>Inness [31]</td>
<td>“…[To] provide the individual with control over certain aspects of her life”</td>
</tr>
<tr>
<td></td>
<td>1999</td>
<td>Etzioni [20]</td>
<td>“The realm in which an actor … can legitimately act without disclosure and accountability to others”</td>
</tr>
<tr>
<td>Control over personal information</td>
<td>1967</td>
<td>Westin [70]</td>
<td>“[T]he claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others”</td>
</tr>
<tr>
<td></td>
<td>1969</td>
<td>Fried [22]</td>
<td>“[T]he control we have over information about ourselves”</td>
</tr>
<tr>
<td></td>
<td>1972</td>
<td>Miller [38]</td>
<td>“[T]he individual’s ability to control the circulation of information relating to him”</td>
</tr>
<tr>
<td></td>
<td>1995</td>
<td>Information Infrastructure Task Force [47]</td>
<td>“An individual’s claim to control the terms under which personal information—information identifiable to the individual—is acquired, disclosed, and used”</td>
</tr>
<tr>
<td>Personhood</td>
<td>1964</td>
<td>Bloustein [10]</td>
<td>Protects against conduct that is “demeaning to individuality,” “an affront to personal dignity,” or an “assault on human personality”</td>
</tr>
<tr>
<td></td>
<td>1989</td>
<td>Rubenfeld [51]</td>
<td>“The fundamental freedom not to have one’s life too totally determined by a progressively more normalizing state”</td>
</tr>
<tr>
<td>Intimacy</td>
<td>1992</td>
<td>Inness [31]</td>
<td>“The state of the agent having control over decisions concerning matters that draw their meaning and value from the agent’s love, caring, or liking”</td>
</tr>
</tbody>
</table>

Privacy covers a wide range of concepts and values. At its core is the notion of “limited access to the self,” which includes solitude, political privacy, and freedom from intrusions by the media and other
entities [55]. Secrecy or concealment of information, and control over information are major privacy issues. Information about a person should be under full control of the person.

The person decides whether to keep the information secret or to disclose it to others. Attaining privacy can also mean rights to aspects of life such as family, body, sex, home, and communications [55]. From a legal perspective, people have a reasonable expectation of privacy, but the definition of “reasonable” lacks consensus and measurement, especially in the digital era. [71].

As knowledge-based services continue to flourish, privacy has evolved beyond the right to be let alone. Individuals should be able to determine when, how, and to what extent information about them is communicated to others [25]. Table 1 above summarizes the development of privacy definitions over time.

3. The Four Dimensions of Privacy

Solove’s taxonomy categorizes privacy for the Internet and digital world into four principal groups of problematic activities [55]:
- **Information collection:** intelligence, surveillance, reconnaissance, and interrogation;
- **Information processing:** identification, security, aggregation, secondary use, and exclusion;
- **Information dissemination:** disclosure, breach of confidentiality, exposure, increased accessibility, blackmail, appropriation, and distortion;
- **Invasion:** intrusion, and purposeful interference.

The taxonomy provides a structured framework for potential roles for government protection of personal privacy, predominantly from a legal perspective. In order for businesses and individuals to evaluate how privacy issues affect service design, influence the decision making process and co-creation outcomes, we re-categorize the activities in the taxonomy as four dimensions of privacy. The breach of the primary dimensions, confidentiality and anonymity may not only harm the personal right of being “let alone,” but also enable further invasion of the secondary dimensions, security and safety. Figure 1 illustrates the scope and dynamics of the four dimensions of privacy.

### 3.1. Confidentiality

The ISO 7498-2:1989 standard for information processing systems defines confidentiality as the “property that information is not made available or disclosed to unauthorized individuals, entities, or processes [32].” Information shared by customers is intended for company use for specific purposes according to the user agreement. This standard is similar to the “need-to-know” principle in the Commonwealth Protective Security Manual which specifies the availability of information should be limited to those who need to use or access the information to do their work [7].

Companies have the responsibility to ensure that customer information is only accessible to authorized personnel. Secondary use of information outside of the agreement, disclosure by intentionally making the information available to third parties through contracts, or unintentional leakage due to theft, intrusion or hacking is considered a breach of confidentiality.

In this strict sense, confidentiality includes the protection from intrusion and the disclosure of private affairs or facts which the owner would be embarrassed if disclosed [25]. Responsibilities assumed by cloud computing, electronic health records, financial services and online banking providers naturally fall into this category. Nevertheless, in social media applications such as Facebook and Twitter, where users can freely upload and share information, facts can be leaked by other users. A picture uploaded to Facebook can expose the whereabouts and behavior of another user who is not aware and does not agree to the disclosure. Geotagging can disclose the location where the photo was taken. Therefore, although service companies provide the platform for the co-creation of value and readily exploit the customer information provided, customers alone run the risk of confidentiality breach by the firms, its partners, other users, and cyber thieves.

![Figure 1. The Four Dimensions of Privacy](image_url)

### 3.2. Anonymity

Generally regarded as the state of being publicly unknown, anonymity includes any personally identifiable information (PII) being protected from public disclosure without the owner’s consent. A European Union directive refers to personal data as “any information relating to an identified or
identifiable natural person, identified directly or indirectly in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity [6][21].” The U.S. government defines PII as information “about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual’s identity, such as name, social security number, date and place of birth, mother’s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information [32].” Anonymity is meant to keep users from being identified or having their information aggregated from different sources as personal profiles. The protection of anonymity is considered the backbone of democracy, which emphasizes the right to self-determination, autonomy, and “free and discreet association.” Anonymity, as political privacy, is a civil right and a core American value [36][59].

Internet user anonymity is eroded by the enabling of cookies, web browser history stealing, device fingerprinting, and other approaches which allow websites to track users’ cyber and terrestrial location and browsing behaviors [15][61]. Fragmented information can be aggregated to create an integrated identity or profile of users and their acquaintances. Online advertising companies, such as Doubleclick (Google), utilize this technology to provide customized, location-based, behaviorally relevant ads to users as they browse the Internet [25].

3.3. Security

Security is a secondary level of privacy built upon confidentiality, availability, and integrity of information [50]. One approach to security is to create separation between an asset and its threat. This is accomplished by moving the asset away physically or logically, making changes to reduce the threat to being harmless, or eliminating the threat [29]. We define security as the protection from the theft of identity, intrusion of personal data and information, and loss in terms of personal property, dignity, and reputation. In particular, appropriation, defined as “the use of one’s identity or personality for the purposes and goals of another,” may eventually lead to the distortion of the user’s identity, personality, opinions and stances, which consequentially cause false representation to the user, damages to reputation, and property loss [55]. Social engineering, such as phishing and baiting, and quid pro quo are common techniques for appropriation.

The need for a security challenge is heightened with the emergence of cloud computing. Secure storage and freedom of accessibility to personal data in the “cloud” is a primary consideration for the continued development of the business model. Unfortunately, security is a key weakness for cloud computing as it invites data theft, hacking, and monetary losses. In the physical world, the security issue may be addressed by requiring customers to produce a government-issued identity (ID) document to verify they are the owner of the account. In the case of cloud computing, the online password-protected system and other complementary “security questions” are supposed to help preserve security and prevent identity theft, but cloud systems are regularly breached to devastating effect [25].

3.4. Safety

We define safety as the condition of being protected against undesirable consequences such as physical injury, emotional and psychological harm, catastrophic financial loss, and life-threatening health failure. The Internet has opened up the physical and cyber accessibility of users, and reduced their ability to control “self-presentation [18].” Individuals can identify other people’s physical presence via the location-based service of their smartphone apps. Employees can be tracked through GPS applications even after working hours [12]. Video streaming via webcams and instant uploads to websites such as YouTube can transmit people’s identities and activities, with or without their consent. Services such as Google Maps and Street View may disclose the presence or absence of a person at a particular location, potentially jeopardizing her personal safety if she is under the surveillance by stalkers and criminals. Children and students starting to surf the Internet and enter chatrooms at an early age can become convenient targets of cyber-predators [15]. Stolen identities, distorted information, rumors, cyber-bullying, and stalking enabled by social media can damage people’s reputation, cause emotional harm, and physical injury. The intrusion of a university student’s private life and sexuality by his dormmate’s two posts on Twitter allegedly led to the student’s suicide in 2010 [17][24].

4. Privacy and Co-creation of Value

Privacy concerns represent a pressing issue for online service providers and a significant threat to future service offerings. It is clearly the reliance on the collection, analysis, and usage of their customers’ personal information that is at the core of the issue. Online service business models rely almost exclusively on revenues generated from targeted
advertising [64]. To better understand this dynamic it is important to understand the roles of customers and suppliers in the co-creation of value.

The service-dominant (S-D) logic of Vargo and Lusch presents a comprehensive foundation for understanding the roles of suppliers and customers in a service relationship. S-D logic redefined the meaning of value and the prominent role of the customer in value co-creation [66][67]. A principle distinction between the goods-dominant (G-D) logic and S-D logic is the type of value created and its manner of delivery [65]. From a G-D logic perspective, services may be offered after sale as an add-on intangible product. This added value is exchanged for compensation, exemplifying the value-in-exchange concept.

Alternatively, S-D logic views service to be independent of products, although products can provision a service [37][67]. Service value, as value-in-use, is always co-created with customers. The co-creation process includes a proposition of value, acceptance of the proposal, and the realization of the proposed value by the firm and its customer through the service experience [56]. The value of a service is no longer considered as being set and imposed by the producer. Rather, it is realized through a value network, in which social and economic actors interact simultaneously [40][41]. The notion of value co-creation represents a shift from the view of the firm that leverages knowledge of its customers in order to create value for them, to one of building capabilities to co-create mutual value with customers [34][56].

How customers and suppliers engage each other in value co-creation can be conceptualized as an encounter process [42]. Encounters can be categorized into three different types that enable the co-creation of value: communication encounters, usage encounters, and service encounters [42]. Communication encounters include marketing communications, dialogs with customers, and collection of personal customer data, whether the customer is aware of the practice or not. Usage encounters involve the customer’s use of the service. This usage is subject to monitoring by the service provider, another form of customer data collection. Service encounters involve service interactions with customer service personnel or online service applications. These encounters are also captured and become a part of the customer’s profile.

It is the data collected and information shared, publicly or solely to the supplier, in the encounter process that is the key to the co-creation of value for online services [71]. Ironically, the very systems that enable value co-creation have raised privacy concerns and trust issues directly related their success in creating value. These concerns are driving the call for more privacy protection. Harmon and Daim presented another side of the dilemma; the usability of service, and thus value creation, would be diminished leaving customers unsatisfied if they are overly protected with constant authentication prompts and other protection procedures [28].

In a free society, people can assume a “reasonable expectation of privacy [55].” Such assumption is the trust built on the assurance and confidence that systems and processes would function as they are set to do in privacy [50]. Currently, users have generally placed trust in the ability to preserve confidentiality, anonymity, security and safety among networks, websites, platforms, operating systems, and apps casually. This is reflected in the results of Hoofnagle et al.’s study of young adults’ attitude towards information privacy, in which they often falsely expect that existing privacy policies are sufficient for protection [30]. Meanwhile, businesses’ ‘reasonable’ behavior is too readily abused [71]. Consequently privacy concerns among customers, recognized as social harms, can affect that shared value between corporations and customers, and create internal costs in terms of privacy fixes and loss of customers’ willingness to share information [44].

As more privacy violations are revealed, customers may question their service provider’s capability to protect their privacy. Even more seriously, customers may doubt their commitment to privacy or question the ultimate motive behind the failure to protect private information. How privacy can be protected while still enabling service relationships to benefit from value co-creation is a pressing issue for future research. It is vital to look into how likely the breach of customer privacy in the primary dimensions would turn into invasion of the secondary dimensions, change the interplay of businesses and customers, and affect the value co-creation process.

### 4.1 Business Value and Customer Value

**Business value** can be defined as the total value received by the enterprise that results from sales of its products and services [58]. Increases in revenue and or decreases in cost result in increases in market position, revenues, and ROI [8][58]. The business value concept implicitly recognizes the requirement for creating customer value; however, its primary focus is creating returns for the firm. Business value tends to be internally focused on short-term solutions for revenue generation and cost reductions that are readily quantifiable. Examples include productivity increases, cost avoidance, cost reductions, discounts, headcount reductions, premium pricing, and
leveraging business assets such as customer information for financial gain. The risk involved with a business value orientation is its short-term focus on profits that can lead organizations to overlook the long-term best interests of the customer, society, and ultimately the business itself.

Business value is conceptually aligned with G-D logic. Products and services are created and delivered to customers as value-in-exchange. The collection, analysis, and use of customers’ private personal data for the purposes of generating revenues from targeted advertising or selling customer profiles to business partners would appear to be purposed to generate business value. The argument can be made that such personal data enable the creation of better products and services and more meaningful experiences for customers. However, no online service providers, especially the social media companies, fully disclose the type and amount of personal data collected how it is analyzed, stored, shared, or otherwise used [71]. Revenues, costs, uses, and risks that result from the use of a customer’s personal data are proprietary to the firm and not disclosed to customers. For the firm, the benefits from using customer data are tangible, financial, and immediate. For customers, the benefits, as they might exist, are intangible and difficult to identify and measure.

Customer value is the “overall benefit derived from a product or service, as the customer perceives it, at the price the customer is willing to pay [27][52].” Implicit in this definition is the necessity for customer engagement for value creation to take place. The degree and type of engagement critically impact value creation. From a G-D logic perspective, a relatively low level of engagement is required. It might involve soliciting customer requirements for new products and services and collecting customer data for segmentation, targeting, and other marketing purposes. Revenues are generated by selling products and services and serving as an online medium for targeted advertising. Market research can be used to assess customer satisfaction. This is a value-in-exchange scenario for co-production of value. Customer value is created, but business value is the primary goal.

From an S-D logic approach, customer engagement is much more extensive and continuous. In this paradigm, co-creation of value-in-use for an online service results from the continuous engagement between two service systems (service provider and customer) to propose, accept and realize value by integrating resources in an open and collaborative manner to create a pleasurable high-satisfaction customer experience [65]. Given the focus on the immediate customer experience, customer value tends to have a short-term focus, co-created or not.

When considering the privacy implications of value co-creation, the G-D logic scenario, with its limited customer engagement, provides less opportunity for acquisition of detailed personal information. The relationship is transactional in nature and customers should be more aware of personal information that they willingly and directly disclose. However, companies can acquire customer information from other sources. Privacy concerns such as confidentiality, anonymity, security, and safety remain at issue. With business value as the primary focus of the G-D logic firm, privacy concerns are limited by the arm’s-length nature of the business relationship.

High engagement S-D logic scenarios that are typified by online social media and search companies make misuse and privacy breaches of customers’ personal information much more likely. Value co-creation should be an open, transparent, continuous, and collaborative process. One might fairly question whether consumers are aware that they are involved in such a process and that their intended or unintended disclosure of private information and personal identity is essential for the co-creation of value, at least from the service providers’ perspective. The online service engagement is remote in nature (on the Internet) with limited physical control of service environment and no physical access to the service provider [43]. A topic for future research would be how much, if at all, confidentiality, anonymity, security, and safety customers are ready to forgo in the value co-creation process. Businesses may also be interested in identifying dimensions that are held more important by customers, and pursuing elements that customers are more willing to give up.

The question is how likely it is that customers consider themselves to be participating in an information market? Do they share the same level of engagement and benefit as the service providers when it comes to personal information and privacy, or do service providers control and benefit most from this information exchange process? Do customers take the time to find and execute the “opt out” option or actually read the terms of service or privacy policy? Does and opt out option even exist? Do customers follow up with the service provider concerning the status of their private information? Do customers falsify personal information or adopt other retaliatory tactics when they view the engagement to not be balanced?
4.2. Free, but Not Free

Traditional G-D logic or “economics of goods” suggests that the value of a product lies within the good itself as determined by the firm [66]. Transactions represent an exchange of money for product or services. It is easy for customers to understand their cost in terms of the price being asked for the product.

However, S-D logic potentially makes it more difficult for customers to align or even identify the costs and benefits of the service engagement. The intangibles such as knowledge, emotions, and experiences created during the value co-creation process are difficult to define and measure [16] [68].

For online services, the “service-for-service” dynamic has become more complex than ever. Many online service providers offer their service for “free” in exchange for user-identified information [28]. Companies such as Google, Apple, and Facebook use this approach to drive their targeted advertising models [64]. To customers, the personal information they give up may seem to be an inexpensive price to pay for the service experience [54]. However, paying for services with personal information is not equivalent to being “free” for customers. The immediate service value that customers receive may be worth less than the long-term value of the personal information that the service company receives.

As customers acquire the service, whether for a subscription fee or “free, but not free” agreement, firms can extract intrinsic business value from customers by monetizing the user’s personal information, without her knowledge or consent.

With online service processes and technologies, the loss of privacy in terms of user information and identification, seems to have become the price tag attached to the “free” services. The “value-in-use” for customers may be overstated while customers cannot be certain of the cost they are paying in terms of what information is collected, its purpose, whether it is shared with third parties for unknown purposes, and how private it will remain. On the other hand, the “value-in-use” for business is more definite and immediate as personal information is quickly monetized through targeted advertising. The social costs of lost privacy can be significant in terms of security breaches, stolen identities, and unwanted marketing communications. The “value” pendulum of service co-creation appears to have swung decidedly to the firms’ benefit.

5. Information Ownership

The necessity for information sharing for the co-creation of value has raised questions of information ownership. Who owns the information? For how long, if at all, are service firms entitled to obtain and retain customer information? How will the new expectations of transparency be realized?

Major privacy concerns and customer anxieties emanate from the exclusion of customers from the right to know about the specific customer data service firms collect, who it is shared with, and how it is used and protected [55]. Businesses lack transparency and openness with their customers and regularly fail to protect their rights to privacy in all its dimensions of confidentiality, anonymity, security and safety as they actively participate in the co-creation process.

Co-creation requires engagement platforms for individuals and enterprises for building network relationships and opportunities for interactions, which in turn reduce risks and costs, and enhance benefits for both parties [48]. This implies a more balanced power between firms and customers in value co-creation. Instead of being offered predetermined value from limited products and services, customers now play a much more active role in the exchange.

However, many customers still live in the G-D logic mentality and do not realize that they are in a co-creation relationship. Users of social networking sites are a captive pool of people who are “monitored like so many lab rats” as targets for precision advertising [64]. They willfully enter value co-creation relationships, readily giving away confidentiality and anonymity, which may lead to serious security and safety concerns.

As such, customers should assess their risks of engagement in the service offerings. They need to gain a better understanding of how the primary dimensions of privacy can be compromised. They may then be more aware of the potential influences on the secondary level dimensions, security and safety, and reconsider their involvement accordingly.

Meanwhile, companies should conduct regular audits of their privacy policies and practices that may invade the primary dimensions, and address potential external threats to and vulnerabilities in the secondary dimensions of privacy, both of their own and their customers.

5.1. You Own Your Own Privacy

Despite the current debates on privacy infringement; business executives, academics, and policymakers concur that privacy and IT-enabled services are not necessarily conflicting goals [59]. The key is to enhance trust and confidence among customers so that they can enjoy the service without compromising their privacy. Opting out of online service applications is difficult for users. Social
pressures and the need for access to news, entertainment, and other information make it almost impossible to abstain from all service providers and value co-creation activities [25]. Some businesses argue that even with more stringent regulations towards privacy and data protection, any new laws may repeat the same measures of seeking consent from customers, who disregard all privacy agreements as a habit [59]. Others point out that since information now flows globally, unified international online privacy and data protection regulations are needed such as opt-in and do-not-track provisions and standards for data security [9]. Before such action is mandated, businesses, customers, government and other stakeholders should arrive at voluntary solutions to the privacy problem.

It is vital for service companies to make privacy an interactive part of the service, rather than a separate privacy notice [59]. Such effort should provide customers with clear and complete knowledge of what information is collected, by whom, for what purposes of, how it is stored, and for how long. In this way, customers can make more informed decisions about their privacy options and settings [59]. It is necessary that firms provide more and specific “opt-in” and “opt-out” alternatives, so that customers can regain control of the confidentiality of their own information, and ensure privacy profiles that they prefer.

Businesses should also demonstrate accountability to customer security and safety by adopting more stringent policies on customer information access and sharing with third parties, such as their marketing partners and vendors, to avoid leakage and invasion of databases. In case of such invasion, corporations should report the incidents to customers and offer solutions in a timely and transparent manner.

Customers, as the ultimate owner of their private information, have the right and responsibility to take charge of their own privacy. A 2010 study indicated that only 14% of the Internet users “often” read privacy policies of the websites they use [30]. They need to transcend from the “operand” mentality and adopt the more proactive, “operant” approach to value co-creation, and understand their potential threats and options. When being introduced to a new service, they need to explore their various functions in greater detail, and evaluate the possible benefits and costs before adopting the service.

5.2. The Right of Future Use
The incentive for new service deliveries by firms is achieving long-term economic growth through the exchange of knowledge and skills with customers, while maintaining the right of future use of such operant resources [68]. However, the mere possession of personal information does not necessarily translate to unlimited and indefinite rights to use that information [25]. If customers become more aware of the operant resources they possess and create, but are not able to determine how long such resources would be retained by the service provider, they may not agree to the exchange, holding the “right of future use” in question. The confidentiality and anonymity breaches by businesses may have a lingering effect upon customers’ security and safety, even after the service is terminated.

6. Conclusion and Future Research
Our review of the issues concerning privacy and co-creation of value for online services has identified some important issues that need to be addressed. In another era, product firms operating under G-D logic principles did not rely on collaborative relationships for co-creation of value with customers. Consumers’ personal data were less at risk, since only minimal customer data was necessary for business operations. With much less engagement between firms and customers there were fewer opportunities for co-creation of value and little concern of privacy issues.

Online social networking and search service firms operating in an S-D logic environment present a much higher privacy risk for customers. The co-creation of value appears to be bifurcated into two parts. First, the extraction of personal data and monitoring of customers’ online activities for business purposes other than the co-creation of a customer value borders on unethical behavior. Most of the income generated by the use of customer data is from targeted advertising, not the service itself. That is very good for business value, but questionable from a customer value perspective. And most importantly, the service firms appear to be unable to ensure the privacy of their customers’ information. The breaches of customer-identifiable data are massive and accelerating.

Second, personal data are undoubtedly being used to improve the online services. At issue is whether or not the customer is actively participating in the process or merely being data mined by the company to determine future purchase opportunities.

In terms of motivating future research, the following issues should be considered:

a. What is the relationship between customer privacy concerns and co-creation of value in S-D logic situations? A case can be made that highly engaging online service relationships provide an accommodating business model for misuse and theft of customer data.
b. Does use of customer data for targeted advertising enhance the underlying online service experience of customers for social network and search services? Or is this relationship unbalanced?

c. What is the true cost to the customer of the “free, but not free” service model? What price would customers be willing to pay for Facebook- and Google-like services if they were only offered on a subscription basis where customers had total transparency and control over the use of their personal data?

d. What role would privacy in all its dimensions play in a conceptual framework for value co-creation such as that developed by Payne et al. [42]?

e. What should the customers’ rules of engagement be for online information exchanges such as social networks and advertising based search? Poddar et al. [43] has suggested variables such as prior relationship with the site, site credibility, exclusivity of the product or service, type of personal information required, criticality of the personal information, invasiveness of the information requested, equity of the exchange, imbalance of power, and customer retaliation likelihood.

f. Finally, a taxonomy of distinguishing factors for the co-creation of value as it impacts customer privacy is possible. Lawer [34] offers the following factors as a beginning: the type of the value created, tangible or intangible; who benefits?; the relative benefits for participants; the explicitness of customer benefit; the ability to define, measure, and understand the value created; the timing of value creation; where and when value created is used in context of customer experience; the relative degree of competence, customer’s value creation skills resources vs. that of the firm; the number and type of customers participating; the customer’s role in value creation, active vs. passive and aware vs. not aware of their role; the nature of knowledge exchanged, expressed, latent, or some combination; the degree of third-party interaction; and who owns the knowledge created?

10. References


