Bargaining for Your Privacy in the Information Age: Systematic Factors Undermining the Equity of User-Company Online Information Transactions

Peter Glazer[1], Jonathan Straus[2]
[1]Portland State University, School of Business Administration, Portland, OR, USA
[2]Portland State University, Systems Science PhD Program, Portland, OR, USA

Abstract–**Consumer privacy and protection of personal information are among the forefront of emerging complex social issues in the internet age. This growing threat to consumers' safety and security is framed as a systemic problem of structural inequality, specifically one where consumers are situated in positions of inferior bargaining power compared to the online service providers they engage in personal information transactions with. We propose a host of vestigial societal factors interacting with the turbulently transitional information-based economy, including outdated legal and economic regulations as well as cognitive limitations and cultural preferences among public users, reinforce and exacerbate these inequitable consumer-company relationships. Potential implications on future policy, social changes and directions for future research are discussed.**

I. INTRODUCTION

People have always had secrets. From time immemorial, there has been value for individuals to keep their sensitive personal information private, restricting the privileged knowledge to pertinent trusted confidants (if any) and safeguarding it from others with whom the information may do the individual or groups harm. The sanctity of personal information is also premised in the design of our modern civil society, which seeks to maintain a dignified, functioning public sphere where professional relationships essential to the workplace are sustained and the private lives of individuals are protected from fear of arbitrary libel in the due process legal system, among other outcomes vital for collective well-being. Ironically, as contemporary social-economic life relies on further differentiation of the public sphere and peoples' private affairs, the accompanying growth of the internet, electronic social networks, and other information technologies entrusted to handle data from both these domains (frequently, between them) complexify their systematic separation. Through home computers and (increasingly pervasive) personalized mobile devices, people routinely exchange personal information with friends and conduct official business with employers, often within a few keystrokes on the same application. While companies offering these electronic services and products trumpet the convenience, entertainment, and distant social connections they facilitate, the benefits to users and collective society are clearly not unmitigated by hidden costs. Built into the infrastructure of the internet, virtually all electronic interactions entail signatures including information about location, time, identity of machines, among other traces that are indefinitely retained on the cloud. Though these features of our electronic media may also be of utility to customers on occasion, they just as easily are accessible by any third parties with sufficient clout, motive or technological savvy. A string of unearthed developments, from the National Security Agency's hacking into citizens' mundane activities (tapping into Verizon wireless activity, and mining Facebook and Google inquiries from as far as a decade back), to careless leaks of personal information tarnishing individual's public/professional images (including photos from old employer databases and dating sites), prompts questions about the risks and dangers to the integrity of private persons' social, financial and even physical well-being. Unfortunately mere awareness of these continued dangers have not been sufficient to engender widespread change in the practices of companies handling personal information, nor induce greater meticulous exercise of privacy precautions in the behaviors/habits of most online users.

This paper characterizes these issues as problems symptomatic of unequal bargaining power between online service companies (which profit enormously from monetization of personal information) and individual consumers (who bear virtually all the risk of compromised information, for comparatively small benefits). We survey some major characteristics of dynamic information-based economies that both conceal and exacerbate inequality in trading relationships/exchanges exploited by large companies, while from the consumer's end, we consider the heuristics by which individual users valuate their personal information against perceived value of services gleaned from companies, and their cognitive limitations/biases in managing their privacy in the midst of exchanges with online service providers and social network sites. This paper establishes a framework around privacy domains, information valuation and equitable information transactions in sections 2 and 3, and proceeds with an overview of the legal and economic incentive structures governing the behavior of firms (section 4) and the empirical trends and dynamics surrounding user attitudes and perceptions about privacy valuation with their counterintuitive impact on users' behavior (section 5). By conceptualizing the economic, legal, and psychological forces that distort these relationships and their dynamic interplay in the larger information market, we may identify leverage points for addressing this inequality.

II. ONLINE PRIVACY

A. Overview of Privacy Domains

Privacy is composed of four essential domains: confidentiality, anonymity, security, and safety [1].

Confidentiality and anonymity are conditions of private information handling intended to promote the individual's safety. While anonymity directly assures safety by disassociating identity from information, confidentiality indirectly facilitates safety through security. Adequate enforcement of sufficient confidentiality policy minimizes the total cost of disclosure, and trust acts as a feedback mechanism established through assurances of safety and reinforced by reputation for upholding such assurances.

B. Confidentiality

Confidentiality involves setting and enforcing rules that limit access to or disclosure of certain types of information. Information shared by customers for a specific use should be restricted to those involved in executing necessary operations [1,2], and unauthorized secondary use or disclosure by the trustee to a third party, whether due to ignorance, negligence, or deception, constitutes a breach of confidentiality. U.S. law contains privacy provisions governing some professions, such as those of attorney-client privilege, physician-patient privilege, and industry-specific privacy regulations [3–6]. Whether protecting the accused from insufficient due process, patients from discrimination, or the safety of the general public from itself, privacy laws exist to extend human justice into otherwise ungoverned systems that would be socially volatile. At the same time, confidentiality may often be legally curtailed in scope to coexist with broader societal regulations, yielding to the overriding imperatives of saving lives, physical safety, or crime prevention. Standard protocols that annul confidentiality in the otherwise private interpersonal domain are common in the U.S., such as mandatory reporting of gunshot wounds to police, impaired drivers to the Department of Motor Vehicles, sexually transmitted diseases to a spouse, and termination of pregnancy to a minor's parents [3,7].

Similarly, for the operation of many online services, certain disclosures are necessary. Unfortunately, new kinds of information disclosure made possible by the internet transcends categories traditionally defined by legal precedent, making it difficult to treat confidentiality between online parties under a cohesive framework and thus remains largely unregulated. In online social networks, poor policies or mismanagement of user preferences may allow unintended or undesired information leakage, but perhaps a more insidious threat comes from networks in which privacy may be violated through others publishing information that implicates a user by association, leaving users at the discretion of their peers and the capabilities of the network. Even the seemingly innocuous act of "tagging" a friend in a photo taken with a GPS-enabled camera device can easily disclose the whereabouts and activities of a user without any direct intent [1,8,9]. In short, confidentiality is only as strong as security policies can ensure, and there is no functional difference between unlimited secondary use, pervasive surveillance, and breach of security even if the intents of sharing information and corresponding method of disclosure differ.

C. Security

Security is the barrier between information and unauthorized parties. It is the role of information security to protect information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. With the modern social-economic pressures/expectations for organizations, businesses, and many connected individuals to establish and maintain an online presence, such parties must employ technical security measures to mitigate the hazards of inhabiting globally public digital space. Servers' privacy protocols precipitously change, user accounts are often compromised, and public websites are frequently under attack by hackers. Specific instances of hacking and the necessity of applications to deter such attacks have been prevalent in recent news. From Facebook to Target and LivingSocial to Evernote, entities that deal with large chunks of sensitive data will be the targets of malicious activity. LivingSocial had the names, email addresses, dates of birth, and passwords stolen for more than 50 million users and note taking application Evernote had to reset all 50 million of their user's passwords after a network breach [10]. In each of these instances, applications such as security layers, a security token, significant firewalls, or sophisticated antivirus and antispyware software may have had the ability to thwart the attack. Network layer security of digitally transferred information can be protected using authentication protocols, working in tandem with cryptography and gateway protocols to establish secure communications between distant systems through a network of relays. When a higher degree of security exists, people are more likely to provide truthful answers and disclose their confidential information over computer-mediated settings [1,11].

Far from mere technical limitations, however, the scope of security may be limited by the requirements of the state whose governing bodies may desire to gain "backdoor" access to generally protected information, ostensibly in response to a perceived crisis. Since 2001, the U.S. government has strongly supported data retention requirements for Internet Service Providers [12]. Additionally, the FBI and NSA have requested current and expired encryption keys from service providers in an effort to unlock secrets hidden in communications collected through these retention policies [13,14]. Recent leaks of classified documentation reveal massive dragnet surveillance programs with some reports indicating that the NSA has even gone as far as to establish a catalog of technical services to infiltrate vulnerable machines and networks [15–17]. Legal tools serve to enforce a set of rules for which technical measures either do not or cannot exist, but laws such as the PATRIOT Act and executive orders citing national security go beyond the scope of thwarting terrorism.

D. Anonymity

The condition of anonymity entails a separation between information and identity. In contrast to security, which relies

on the increasingly sophisticated slew of technological measures, anonymity is a simpler (albeit radical) approach to information handling by preemptively disassociating the signal (be it intimate information, political opinions, or critical/loaded questions) from the source that might otherwise be prohibitively embarrassing or incite retaliation from parties with a conflicting interest to the informant's. Anonymity is critical to learning and developing as a human being, as constant supervision can have deleterious effects on behavior and growth. For instance, children attempting to solve problems will try more novel, creative, and unorthodox approaches when they think nobody is watching (sometimes with surprising results). Similarly, anonymous acquisition of information is hallowed ground in higher education because it allows students the freedom to learn without the expectation that knowledge will be used in any particular way or even at all [18]. Furthermore, childhood and adolescence have always been a time for making mistakes, learning from them, and building experience. The persistence of information in the digital age may pose an inescapable connection to one's past with the most extreme solution being a complete and total identity substitution [19–21]. Nevertheless, despite the key role anonymity plays in protecting individuals from association, anonymous routing service Tor has been viewed from different perspectives as being both virtuous for empowering whistleblowers with a tool to reach media outlets and culpable in facilitating information transmission between those with malicious intent who wish to commit criminal or terrorist acts.

E. Safety

Safety is the ultimate goal of responsible privacy policies, which is the protection of users disclosing information from consequences that may be considered undesirable. These consequences can come in physical, social, financial, emotional, or occupational capacities; additionally safety can be thought of as control of recognized hazards to achieve acceptable levels of risk. While anonymity and secured confidentiality are the major means by (or degrees to) which association between data and identity is controlled or hidden, safety refers to the net resulting risks and scope of hazards for the actual person behind the virtual avatar [1]. While improving security or attempting to build anonymity into a system may generally improve safety, the relationship between these domains is not necessarily synonymous nor straightforward. To illustrate this vital distinction, many websites and services, in upping their security measures, may unintentionally attract more hackers (especially recreational hackers) determined to crack security protocol, paradoxically reducing the overall safety of a system. In short, maximizing online safety involves minimizing the personal risks associated with using the Internet and vulnerability to computer crime in general, and an intelligent concerted application of both anonymity and confidentiality measures with regard to the pertinent dangers are critical tools in protecting individuals from threat of abuse and targeted attack.

Indeed, many threats to safety exist, in their widely varying manifestations. Most of them are exploitative, commonly involving remote parties that attempt to obtain financial information from users by many means, seen in the litany of phishing scams, fraudulent emails, and fake websites (posing as a legitimate service provider the user typically logs into) intended to capture users' bank information. They may be more indirect, capturing personal information of users (as the case of websites that track consumers' surfing habits), using anything from simple cookies to more sophisticated 'spyware', to targeted ads that may entice the users to generate revenue 'clicks', or subsequently sell the information to other third parties for marketing purposes. However, the motives of malicious actions are not necessarily limited to being financial, material, or even logical, but may instead seek to inflict harm on certain users for harm's sake, whether arising from the whims of sadistic amusement or impassioned spite. An infamous example, "Revenge Porn", involves the non-consensual distribution of sexually graphic images of an individual [22]. In the most common cases, a vengeful ex-partner or malicious hacker transfers still images or videos, often originally taken with consent and the intention of remaining private, and supplies them to a website where the public at large can view them. To compound issues, because revenge is the specific intention, often times these submissions come complete with personal credentials and information such as name, family, employers, and peers. Victims have been assaulted, harassed, fired, forced to move, and in the most dire situations, committed suicide [22]. Permissive privacy policies can facilitate costs such as identity theft, stalking, and legal trouble [23]. Cyber-stalking involves the use of electronic media to stalk or harass an individual, group, or organization. Physical presence can be identified through the use of location-based services and GPS applications. Exploitation of such knowledge can result in surveillance, harassment (e.g. defamation, accusations, and threats) and extreme behavior such as identity theft, damage to data and equipment, or even bodily harm. In especially disturbing instances, this vulnerability can lead to solicitation and exploitation of minors and other predatory behavior. It is for these reasons that online safety is very important for parents, as children are more susceptible to deception.

Safety can be improved by taking preventative measures and making an effort to be educated and informed. Minimizing information sharing, maintaining strong access credentials, employing meaningful security, and reserving an appropriate degree of vigilance are all effective tools in thwarting common threat vectors and maintaining an acceptable level of safety. Success in maintaining safety usually manifests as reinforcing feedback known as trust. Trust then manifests as the willingness of one party to rely on another such that they relinquish control over risk, cost, or even harm and events which have a particular degree of uncertainty as to the outcome [1,6,24,25]. Trust entails a

belief in honesty and reliance on others to act in accordance with their stated intent. Research has found that trust levels are particularly influenced by perceived handling of private data, specifically when it comes to online trading systems and attitudes towards online purchase considerations [26–28].

III. INFORMATION VALUATION, EXCHANGE AND EQUITY

A. Information as Value Commodity and Tool

The old adage "knowledge is power" continues to grow in relevance, as the availability of information and means of using it have expanded with the technological developments of our aptly named "Information Age". There is value to be extracted not only from the collection and usage of information but also in propagating it further [29] thanks to the ease of such sharing facilitated by the Internet. While the Internet was introduced to the public as a means to archive and communicate formal knowledge (such as scientific research, expertise on sports, pet care, cooking, etc.) it is also increasingly a platform by which data is pervasively collected from users (whether as individuals or aggregates) to predict trends, from predicting customers' purchasing habits to transmitting fashions and fads, analyzing financial markets or political developments in a rival party, amongst innumerable other applications. This is routinely done passively and automatically, from from obvious social network examples such as Facebook and Twitter to technology giants such as Google, Microsoft, Apple (who mine personal information from interactions and search) as well as information services like Intellius and Spokeo (who aggregate and perform more specialized analyses of meta-data for big clients' use).

The diversity of uses for information and types of goals that it accordingly facilitates warrants a general framework from which goals are broadly distinguished and its value may be derived or determined with respect to its contributions toward said desired ends. Literature in goal framing suggests that parties may have any combination of hedonic, gain or normative goals, each which may warrant different analyses [30]. Hedonic goals pertain to self-gratification in the present, have strong ties to emotion, and tend to have the greatest influence on individuals' impulsive behaviors. Gain goals can be framed as calculated long-term self-interest that is primarily concerned with the persistent, cumulative acquisition of latent rewards such as material resources or money. And finally, normative goals, which are derived from external forces such as public opinion, social pressures, and common moral sense, traditionally play a background role that surfaces in the absence of more direct hedonic or gain goals. Thus, individual users may be driven by hedonic ends to consume the latest internet content (e.g. gossip or cat videos) by surfing a website or social network, while the companies that control access to said content may operate on gain goals, related to collecting a steady stream of revenue or personal information provided by the content user. Collectively, parties that co-create larger societal value in this way (stimulating the economy, expanding the scope of entertainment/recreation, etc.) are presumed to contribute to normative goals. Since these online partnerships are symbiotic relationships (with the user supplying information that creates value for company investing in social or technological platform improvement), a central problem, thus, is how users who provide in fair (i.e. equitable) ways when these goals are difficult to compare and quantify.

B. Transactions, Bargaining and Equity Theory

It is through transactions that people exchange value with each other, whether business to business (B2B), business to consumer (B2C), or consumer to consumer (C2C). If a minimum value for a transaction cannot be satisfied for all parties, then the transaction will fail to take place. Conversely, a transaction should succeed if an acceptable outcome is perceived by all parties involved [31]. By the definition of value, in order for the transaction to take place, the cost must be (or at least believed to be) less than the benefit. The cost of information disclosure is rarely zero (but can be negligible), and it is left to the individual's discretion to decide what institutions, companies, and people can be trusted with what information. Given the multiple perspectives of interested parties, there is interest in negotiating transaction terms and their dynamics because all value creation is made up of transactions, all transactions are made between two or more entities, and studying the fundamental interactions can provide insight as to where leverage points exist. The process of negotiating the terms of transaction or exchange is commonly referred to as bargaining. A wide range of studies seek to categorize and quantify the process of bargaining between multiple entities. From studying the effects of bargaining between suppliers and consumers [32] to the role of information asymmetry [33] and effects of communication [34], bargaining power is influenced by many factors. The theory and application of bargaining strategy as well as the underlying principles (e.g. power, knowledge, and communication) can be used to improve both the total surplus and distribution of value created in a transaction or series of. From start to finish, bargaining begins when one party proposes a bid for exchange with another, continues as the party that receives the bid may accept or reject it (often offering a counter-bid) and so on until both parties are satisfied with the terms and commence exchange or remain dissatisfied until they terminate negotiations [35]. Embedded in this bargaining process may be an economic game where players attempt to retain the benefits of cooperation with the transaction, while strategically trying to maximize their own interest within the agreed-upon terms of exchange [31,36–38]. Parties may, for example, downplay the value of their partner's offer (or overplay theirs), or even invoke levers of power they may or may not actually possess, thus yielding concessions through varying means of modesty and credible threat. Equity Theory suggests that if the outcome relationships are similar (i.e. allocation of value is perceived to be fair), then the exchange

will be interpreted as equitable, and inequitable relationships will be perceived as distressing [39]. Distressed relationships tend to self-correct [40], either by restoring equity to the relationship or by avoiding further inequitable exchanges, so if a customer perceives that ending a business relationship will eliminate distress, then it is of greater interest to the business to salvage the relationship before it is too late. Occasionally, even when the equity of the agreement is imperfect, parties will concede points for the sake of time or fear that negotiations will break down [41]. Pictured below (Figure 1) is a causal loop diagram illustrating the classical theoretical (if highly idealized) self-balancing bargaining process as it applies to the exchange of user information (or funds) to use an online service, where any undue exploitative attempt by the company is unviable in the long-term because it creates customer distress, which must either be alleviated by concessions of greater service on the company's part, or by termination of the trade relationship which would entail a loss for the company and the consumer (in the absence of alternative competing services).

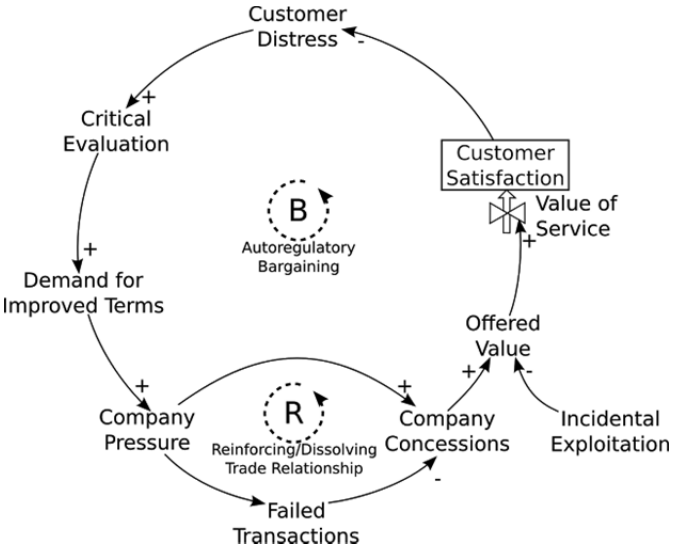

Figure 1: Classic Bargaining and Distress Mitigation Model

However, a key component of this dynamic is information about the larger market, which often dictates or becomes the deciding factor for the course of action (or inaction) taken in the transaction by the participating agents affected by such knowledge [42]. If every party involved in an exchange shares or has the same available knowledge regarding the transactions and values of exchange items, then the process is referred to as bargaining with symmetric information. In research, this tends to manifest as all parties knowing all possible information relevant to the transaction [43,44], and as such responding optimally to each other, the implication being that if individuals perceive greater costs or risk to disclosing their information, they will attribute greater value to their privacy and respond accordingly [45]. If neither greater reward nor reduced risk is offered, then the cost of participation will diminish the value of the transaction and may impact the equity relationship. Whether or not satisfaction will drop beneath some threshold that inhibits further exchange is situational. Regardless, the potential consequences of misuse of information combined with the respective likelihood of misuse actually occurring serve to approximate the actual costs. The extent to which information can be propagated and used in an undesirable way should inspire individuals to demand value when deciding whether or not to disclose information to any party [45,46].

C. Information Externalities and Inequity

The transaction environment engendered by the Internet and characteristics of information as a largely intangible good produces many unprecedented effects (some of them counterintuitive) on the dynamics of exchange and equity establishment. Traditional barriers to market entry, specifically startup costs, proprietary information, and infrastructure requirements are constantly being broken through by online service providers. Even with variability between their quality, offerings are becoming ubiquitous at a rapid pace, changing the value proposition from the individual's view point. If, hypothetically, no costs to disclosing information existed for the user but the user could not capitalize on its value without a second party, the direct value of the information for the user would be nil, but secondary value could still be derived indirectly by establishing an exchange relationship with a second party. From this perspective value is co-created by users and service providers [47,48], but the value of the contributions is often not accurately realized by both parties.

Online transactions offer the user an unprecedented amount of intangible goods. From free email accounts to social network sites, companies offer users social benefits such as the ability to connect and communicate with each other, organize and plan events, and share information, allowing them to compensate users for volunteering their personal information without direct financial expenditures. This is the model used by most social networking sites. Based on the three systems propositions in Social Exchange Theory (success, stimulus, and deprivation-satiation) [49,50]. Value is co-created by users and service providers on an electronic platform that integrates the individual's preferences with a community of photos, comments, and status updates and may also include interaction with apps, games, and advertisements [47,51]. In addition to social benefits, companies also offer entertainment value through games, applications, and access to media such as music, movies, and sports. These offerings can be secured at a discount (e.g. hosted from a partnering high-tech firm's servers), developed in-house, or community- or crowd-sourced (as seen in the user-generated content of said social networking sites), ultimately costing the company little to nothing. Units of value are relatively arbitrary, but the perception of reward will induce behavior, and reciprocity between parties serves to reinforce similar behavior in the

future (Fig. 1). Reinforcement can occur in a number of ways. Depending on the situation, outcomes for the individual can manifest as rewards and costs of varying degrees: For example, fulfilling immediate goals may be accomplished by exchanging information for such rewards as being granted access to a service (e.g. Facebook), discount and promotional offers (e.g. Groupon), or financial compensation (e.g. mTurk). Some businesses may even present value in the form of negative reinforcement by reducing costs [52]. Depending on the site, users can disclose a variety of different types of information, as well as maintain piece-by-piece control over the information's accessibility [53].

However, when disclosure of personal information is involved without strict actionable confidentiality conditions, the transactions are rarely limited or confined to the private user and company, as other, third parties may also seek value from the individual's information. In this information exchange framework, a third party is any entity outside the dyadic bargain (whether individual, company or agency) which sees value in acquiring information from an external source, and their utilization of information initially acquired by the company is considered secondary use (see Figure 2).

One common and constantly evolving business model is to accumulate and resell data, as there is vast potential market for secondary use to create systems for analysis, interpretation, and operationalization of current and future data sets [54,55]. It follows that the behavior of a third party is also relevant to the value of privacy, as actions and secondary use influence the costs to the first party and effect limits on information handling and disclosure. How exchange transpires in the real world depends on many factors including the perceived value of personal information, the costs associated with secondary use, and the probability that secondary use will occur. While it ultimately rests on the individual to decide what information they should disclose and to whom, once it is disclosed, the proverbial cat is out of the bag; it is no longer within direct control of the individual to inhibit further disclosure [56]. Because the risks of secondary use from disclosure are almost fully burdened by the individual and independent verification of usage is nearly impossible, the model can almost be equated to a lemon market [57]. In a lemon market, the uncertainty of quality on a per item basis devalues each item independent of its actual condition. Assuming that individual agents will take note of this phenomenon, the logical step in the bargaining process to facilitate more disclosure is building trust [58,59], as it helps to alleviate this lemon market mentality. Trust is built through repeated, reinforcing interaction. Trust and repeated interaction form a positive feedback loop (at least until one party defects). If no defection occurs throughout the relationship, previous interaction and trust building activities increase the likelihood of disclosure.

Some assurances and consumer strategies exist that substantially this risk (and thus major costs), although at the same time, deprive the company of the full desired value. By itself, an individual's name offers little reward on which to capitalize, but when input into Facebook's service, it can create value for the individual by offering social connections and interpersonal communications in addition to value for Facebook by enabling supply of more information to operationalize. If users do not perceive any costs to disclosure (even if they exist) and there is no other significant barrier to disclosure such as inconvenience, then acquisition of information becomes trivial because virtually any reward offered will be sufficient to induce disclosure [60]. As such, the Android marketplace is an excellent example of readily available substitutes. While most applications request access to as many special permissions as they think they can get away with (storage, system tools, location, network communication, personal information, accounts, development tools, hardware controls, and network communications are necessary for Google Chrome), functionally similar ones are often available with fewer, if not void of, said permissions. This increasing competition has the ability to induce marginal increase value in offerings, in whatever form the parties come to voluntary agreement on [61].

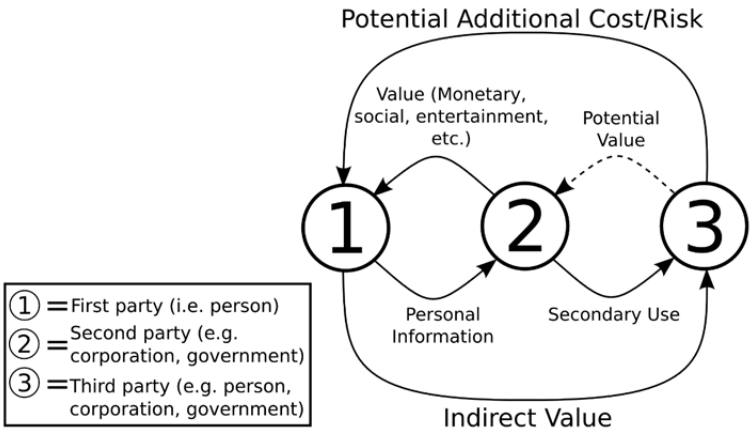

Figure 2: Inter-party value exchange

Thus, by virtue of information-based transactions being typically repeated interactions through the relationship, there is often plenty of opportunity to fine-tune terms for the next. This is especially true of intangible goods, and information is precisely that. Online social networks involve a series of information transactions, and since bargaining strategy can be employed for every transaction, a change in policy can be considered a value proposition in the negotiation stage of a transaction. In 2009, Facebook's policy change shifted their privacy stance from one based on group-level privacy to one that grants Facebook virtually unrestricted use of any and all user-submitted information [62,63]. As a result, user response has been varied, from generating strong feedback from vocal users to inhibiting the use of services by less expressive customers. Nevertheless, users are more and more frequently finding themselves juxtaposed against market forces that seek to monetize information through secondary use, often at their expense. By allowing more frequent updating of terms, it also enables users defect from a company more quickly. Let it not go unheeded that users can and will defect away from a company, even one they have associated with for years. Despite a large customer base, social news aggregator Digg saw both prodigal rise and catastrophic fall in the span of about six years. From its launch in 2004 until the latter half of 2010, Digg saw a boom in popularity, followed by repeated backlash from mismanagement, and eventually a mass exodus of users [64]. In 2006, Digg was in negotiations with Google to sell for around $200 million, but a mere four years later, it sold for $500,000. Today, Digg exists as a perfect example of the potential consequences of user response to insufficient value [65,66]. On the flip side, if the inequitable distribution of surplus is met with ongoing transactions, it's likely the party in distress is facing some type of cognitive bias that prevents objective analysis, resulting in a delayed, much belated response to the exploitative relationship if the abuse happens to even be discovered (see Fig 3).

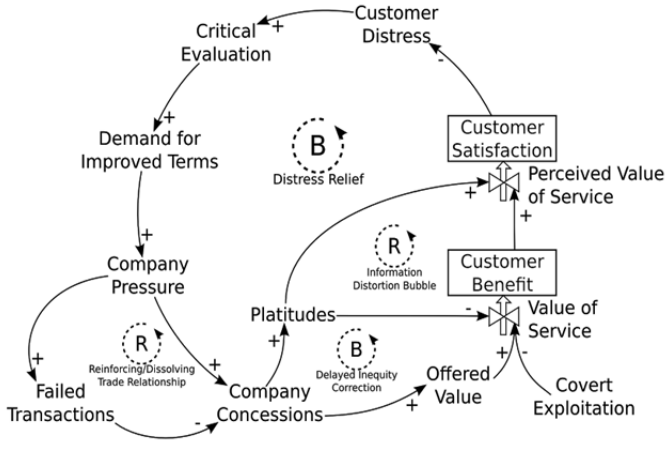

Figure 3: Bargaining Model with Imperfect Information and Third Party Externalities

IV. ONLINE SERVICE PROVIDERS

A. Factors in Company Decision-making

As discussed in the previous section, the firms that provide online services are a chief party in most online transactions involving formal disclosure of personal information, and merit serious consideration as major players by the systematic advantage many gain by exploiting information asymmetries in the market outside the scope of legal recourse. Being largely indifferent to the directives of normative goals, the factors constraining the actions of online service providers are thus considered to be almost exclusively legal and economic. Such firms are likely to identify value primarily through financial capture, and socioeconomic events such as a successful advertising campaign or bad publicity are examined from the perspective of their bottom line. With money being the first, foremost, and sometimes only factor that affects corporate behavior, it is advantageous for businesses to maximize their value capture, only paying heed to legal ramifications when their penalties exceed the opportunity cost of bypassing a regulation. This type of strategy is frequently seen in firms (as in the case of some large financial institutions like Chase bank) that may permit recognized illegal accounting practices, with executives recognizing the greater cost of retracting the violating action. However, whether that means extracting as much value as possible in every transaction or adopting a strategy that yields some initial loss in order to capture future value reflects wisdom and shapes behavior may be sensitive to contexts and operating assumptions of executives.

In fact, even within the framework of profit-maximization, the actual behavior of companies is not rational. This phenomenon occurs because of the constant push and pull struggle between long-term motivations and short-term incentives being out of alignment. Because the most influential stakeholders in a for-profit institution are the shareholders, even when a company is motivated to abide by long-term gains, they are incentivized to profit in the short-term. Frequently enough, the only thing stopping the societal race to the bottom that defines the competitive marketplace are imposed costs in the form of legal ramifications. Even directly acknowledging that most clients have significantly more value when treated as an ongoing relationship as opposed to the sum of their transactions, online service providers are guided by short-term profit because of the conflicting personal and entity issues of the individuals responsible for daily operations [67,68]. Many service providers have built large initial customer bases with free perks, but end up losing them (sometimes before they have recouped the cost of acquisition) partially because they underestimate the lifetime value of the relationship and partly because of uncertainty regarding the quantifiable value of the lifetime relationship. If a company cannot quantify the value of future customer interaction, then it may assume that the value is zero and that the present transaction constitutes the

lifetime value of customer retention [69]. This perspective also arises when future value is jeopardized by economic survival. As money is the lifeblood of an economic entity, a company in financial distress may adopt a suboptimal long-term strategy if the potential for survival is even remotely threatened or in jeopardy.

B. Market and Regulatory Failures

The result of this internal struggle and resulting tension with external market demands is that service providers will do anything in their power to create and capture as much net private value from each transaction as is possible, without regard for the value added from their service, or costs to society (careless handling of public user data or otherwise violating users' trust and confidentiality) while sheltering themselves from the wide-ranging consequences of such negative externalities. This dilemma, so eloquently explained by the tragedy of the commons archetype [70], perfectly exemplifies the importance of legal sanctions as a safeguard against the abuse of corporations. While centralized, narrowly targeted regulation emphasizing innocence until proven guilty (adding prohibitions only on a case-by-case basis) makes sense in many spheres of public life, empirical evidence shows that governing bodies, legal statutes, and precedents have not kept up with the proliferation and evolution of technology [71]. In the absence of legal recourse, the only cost to companies of secondary misuse is customer response and reaction. In 2000, the Federal Trade Commission sued to block bankrupt e-commerce retailer Toysmart.com from selling its database of customer information against the terms of their own privacy policies [72,73]. The case settled with the database being destroyed but without setting clear precedent for similar cases in the future. The fact that there is even a question as to whether the information, separate from its encumbering policy, is a company asset to be auctioned off to debtors means that there is potential for value extraction through unauthorized secondary disclosure in similar legally-ambiguous situations that go unenforced and perhaps even unnoticed.

As if potentially conflicting internal goals and lack of proper oversight in hard legal cases aren't issue enough to deal with, the inchoate regulatory structure of the market such as Success to the Successful (or "Rich get Richer" effect) reinforce first mover advantages and create even further incentives and perpetuating factors that bolster the value proposition of the firm, all which are particularly prone to manifesting or being magnified in a virtual information-based environment with no tangible material constraints. Mechanisms such as Preferential Attachment [74] ensure that large social networks (such as Facebook) will continue growth by virtue of the existing number of users. That is, the value proposition offered to each subsequent user is proportionally increased by the previous user's adoption. Similarly, a reinforcing factor of technological adaptation, ensures that other virtual platforms wishing to interface with existing users build their technology to be compatible with pre-existing standards established by dominant social networks from which communication is reliant [75], further "locking in" subsequent users and the online community as a whole into a paradigm regardless of how objectively good that hegemonic design may be against protracted competition (which has been argued is the reason why the QWERTY keyboard is dominant despite objectively more ergonomic layouts, and Microsoft applications are still par for most major workplaces and schools). These phenomena hinder what otherwise might be superior platform technology or terms of service from a different offering due to high costs of switching, lack of organization among individual users [76,77], and overall inability to hit the critical mass or tipping point required to achieve mainstream adoption. In turn, this inhibits competition, which is the necessary ingredient for any large-scale market to sustain stable, continued standards for consumer service and bargaining leverage. Given the lack of avenues for individual legal resource, the monopolistic or oligopolistic nature of the information economy, and the general bias towards making shareholder as opposed to stakeholder interested decisions, current conditions practically guarantee the growth of online service providers so powerful and pervasive in their ability to influence and facilitate ongoing disclosure [78].

Thus, contrary to the intended purpose of legal regulation, which is to inhibit or regulate behavior producing gross negative excesses, the legal infrastructure has been subverted in a explosive sweep of regulatory capture [79], creating a legal process whose inherent ambiguity becomes pliable, while costly and tortuous to navigate for the users claiming actual victimhood. Political lobbying, local monopolies, and retroactive modification of policies are examples of legal tactics for companies to extract value from their customers, society, and the system as a whole. Facebook is but a single example of a big company trying to steer the future of online privacy [80]. Apple and its iPhone devices integrate with services that provide location tracking and remote control. Google has been steadily expanding since its beginnings as a search engine, branching into email, acquiring online video service YouTube, and expanding further toward cloud services such as documents, files, music, TV, and movies [61]. The ongoing modification of privacy defaults can be interpreted as a change in the transaction terms of the bargaining game; ergo, changing policy is a bargaining strategy to capture greater value. And, unless the new policy allows users to revert their settings to behave like the previous policy, they are left with a dilemma: accept and continue participating or reject and defect (e.g. to a competitor or by limiting disclosure). In the absence of a more direct communication channel, the act of rejecting an offer serves as the only available balancing feedback. As a result, there has been much latitude for increasingly slanted privacy policies [81]. In its inception in 2004, Facebook's default privacy settings were on the conservative side of permissive, but nine years and several revisions of the site privacy policy later, Facebook's default settings lean toward

dystopian transparency. In 2009, their privacy policy was revised to make friend lists publicly viewable across the site and, despite heavy criticism from the Electronic Frontier Foundation and American Civil Liberties Union, within a month it was adopted. Most of the settings now default to visibility by anyone on the Internet [62], [63].

V. USER COGNITION, PERCEPTIONS AND ATTITUDES

A. Individual Decision-making

As naturally social creatures, human utility drivers extend beyond mere direct and indirect financial compensation. Instead, normative goals direct value deriving behavior with regard to customs, traditions, and other social pressures. Given that financial gain is the only compensation to online service providers, recognizing and operating within defined constraints is particularly easy when the only guiding parameter is the legal boundary. As more than legalistic beings, we are forced to make pragmatic but potentially suboptimal decisions regularly because of our incorporation of additional factors beyond supposed black and white legal restriction. That is to say, we as humans make decisions out of not just financial benefit, but of our intuitive sense of right and wrong.

B. Heuristics of Valuation and Social Cognition

People navigate the complexities of decision making through heuristics and/or shortcuts. While they are generally effective in daily social interactions and practical situations, they can lead to anomalies when compared to selfish, self-interested, or self-maximizing behavior, thus violating the assumed and generally accepted theory of Homo Economicus. That is, we do not tediously calculate optimal outcomes for all decisions, rather we use prior proxies to determine useful behavior.

Exemplifying individual's tendency against switching, there is a major discrepancy between the price at which one would sell a good they own and the price they would be willing to acquire the same good in the market. Tested empirically with a simple coffee mug, evidence showed that the amount someone required to give up an owned product was often more than twice what they would be willing to pay for the same product they didn't own [82]. Classical explanations of prospect theory and the endowment effect help explain this discrepancy; when coupled with the view of online service offerings being co-created with the provider, significant overvaluing of these service offerings occurs [83,84]. These biases have major implications on our everyday interactions and behavior towards default brand loyalty, as people are both motivated to stay in long-term economic relationships because of lavish, unconditional perks, and because the cost of switching is high. In essence, it's difficult to justify changing behavior when it create both direct and indirect costs.

Similarly, the time value of money (i.e. a dollar today is worth more than a dollar tomorrow), while not difficult to understand as a concept, requires the assumption the investment made will go up. However, the nuance of being able to correctly judge risk and reward from a net present value perspective is an acquired skill. Similarly, understanding and reconciling the hedonic bias (immediate gratification) as a distortion that overvalues "today" and undervalues "tomorrow" helps explain the privacy bargaining scenario [85]. Coupled with this distortion and the costs of switching, once a user or group adopts a particular platform for their service needs, they can become intertwined in an exchange relationship that is or seems equitable early on, becomes or is perceived to be distressed later, but still cannot be broken out of. Google and its respective services are a prime example, as the customizability of certain features and nuances makes it more tedious for users to switch to decoupled or alternate services [86].

The idea of individual human rights and dignity in contemporary western culture constrains the types of transactions that people are willing to engage in online. They may reject the terms of an invasive privacy policy outright on principle (moral intuition) and will be less likely to be intrusive on their partner's privacy on moral premises. Furthermore (as emphasized in Social Exchange Theory) perceived equity is a vital criteria in terms of exchange relationships. In contrast to the behaviors assumed of the "rational" self-maximizing entity, behavioral economic experiments show that individuals will reject inequitable offers, even at personal opportunity cost [87]. In an experiment where workers "discovered" they were being paid different amounts for the same work, even when the work was easy and overpaid for to begin, all of the subjects paid less than the remaining participants refused to participate and left [88].

C. Attitude and Perceptions of Fairness

While highly intertwined, attitude and perception are not exactly synonymous. Perception is one's belief of how reality exists, where attitude is the belief about how reality should exist. Attitude is crucial to explaining the individual's decision making process. If one's belief about what the equitability of a transaction should look like does not match up with their perception, an exchange relationship cannot be stabilized. Where perceptions are dependent on information available to the consumer, attitude and fairness retain room for subjectivity. This inherent subjectivity creates situations where one person might think it is fair or even favorable to give up information for some reward if they primarily value the reward that the company can provide while another person may be principled against disclosure, seeing it as a threat to confidence, regardless of the actual danger to them or benefits entailed in a hypothetical online transaction [89]. As exemplified below (figure 4), attitudes are prone to being adjusted based on experiences and, in order for the transaction to continue, customers must find a way to restore equity, artificially or otherwise. One method for this artificial restoration involves the Just World rationalization, in that individuals justify a situation as "the way it is" without conceptualizing an alternate scenario [90].

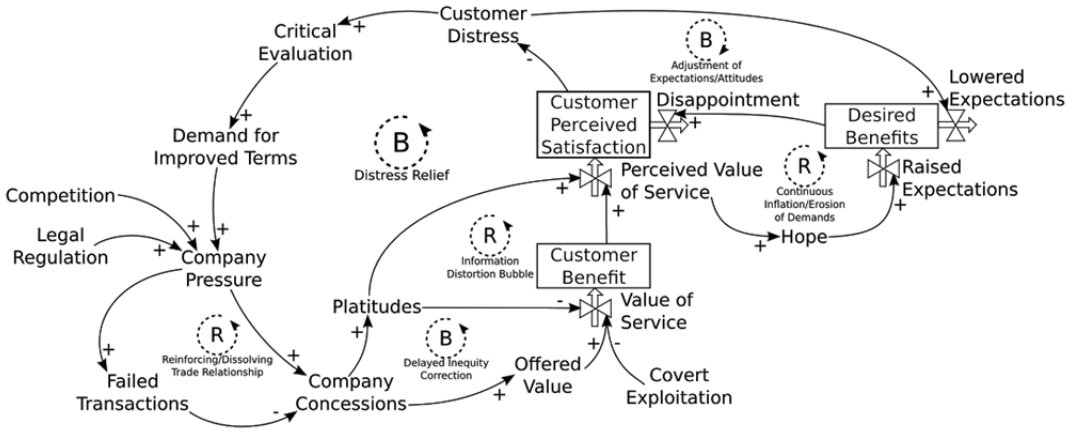

Figure 4: Augmented Bargaining Model with Company Incentives and User Attitudes

D. Risk Perceptions and Transaction Behaviors

In a 1999 study, survey responses of 381 U.S. Internet users displayed a high level of concern about general Internet privacy, with only 13% of respondents reporting to be 'not very' or 'not at all' concerned [91]. Respondents were classified into three main categories: "Privacy fundamentalists" (17% of respondents) were extremely concerned about their data use and were generally unwilling to provide any data to websites, even when assurances were given to protect privacy, the "Pragmatic majority" (56% of respondents) who were more willing to partake in certain transactions as long as their concerns were acknowledged and addressed, and the remainder "marginally concerned" (27%) who were generally willing to provide data under almost any circumstance with minimal formal assurance of their information safety [92,93]. Consistent with this tendency towards moderate attitudes, a subsequent study by Westin a mere two years later found 26% of respondents considered themselves to be fundamentalists, 64% pragmatists, and only 10% identifying as unconcerned [94].

Results showed people's attitudes toward most items varied greatly regardless of reported general levels of privacy concern, although even with the segregation and clustering techniques used, four attitudes were consistent throughout categories: 96% of respondents stated that secondary use of their information was either somewhat or very important, with 79% claiming the latter position [91]. Hence, at least in principle, people are almost unanimously concerned with the secondary use of information. Three other criteria were considered significant but not distinguishable across groups: the type of information collected, the purpose for the collection, and the ability for said information to identify individuals. Upon analysis of feature utilization, a study on the privacy implications when using Facebook discovered that while more than 5/6 of surveyed are aware of their ability to change their privacy settings, less than 1/2 made any changes from the default setting [95]. Two final results and points worth noting: First, simply knowledge of an existing privacy policy was not enough to convince individuals to partake in a transaction; rather, it is important to know what the policies are [91]. Second, there is a lack of concern for knowing what a company's data retention policies are. Comments imply that, without some sort of verification, it is useless to believe companies will actually purge their databases of personal or other user-specific information [91] making it appear that apathy, not paranoia, is often the response to lack of information or policy ambiguity.

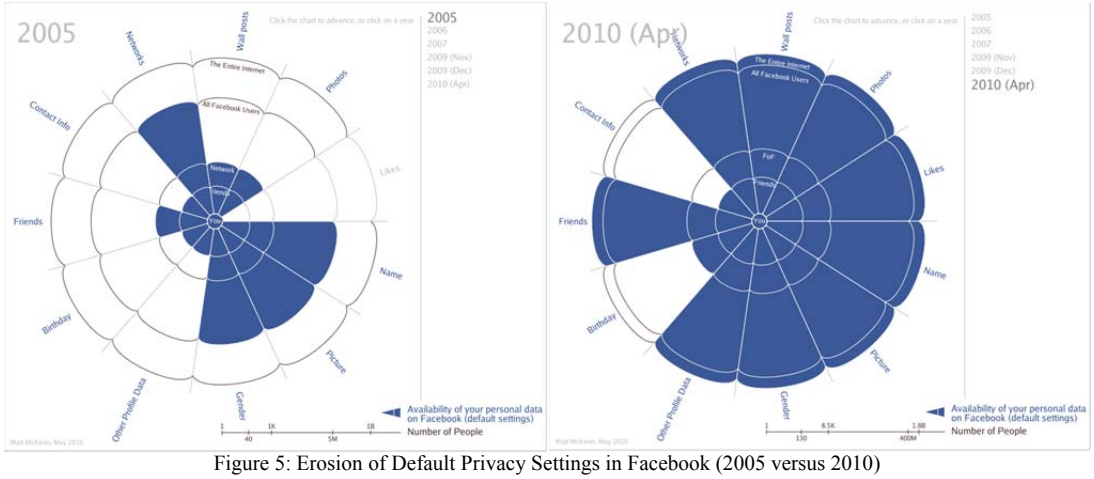

Figure 5: Erosion of Default Privacy Settings in Facebook (2005 versus 2010)

VI. GENERAL DISCUSSION

While the Internet and the constantly expanding, evolving information technology powering its services to users from around the world hold great promise and potential for societal benefit and enjoyment, entailed in its sheer scale are risks of uncertainty/instability, opportunities for abuses, and unprecedented scales of disaster and loss. Broad observations highlighted in this paper paint a troubling picture of most value being realized and capitalized by companies, while a disproportionate share of its perils and risks are systematically absorbed by individual customers who typically have no say in the decisions or company's policies producing the dangers, or even detailed knowledge of them. The power and influence accorded to online service companies are justified by the hypothetical value they presumably add to society (through the social/business connections they facilitate between users, dissemination of knowledge they promote, or new forms of entertainment they provide), but like any for-profit businesses with stockholders, have a primary imperative to maximize private value capture, regardless of negative externalities (even if they negate and exceed any net benefit to the general public). Coupled with the lack of legal incentives and other formal consumer protections in online transactions as well as the monopolistic/oligarchic nature of technological adaptation, adversely affects the quality of services that are actually available to most consumers. Furthermore, human users in these online, intangible, information based economies behave far differently from the idealized, "rational", utility maximizing individuals assumed by neoclassical economics, faring poorly as competitive bargaining agents. In the absence of sufficient information in the Internet's cacophony of information, people typically underestimate the monetary value of their personal information, assume trust in repeated actions, and on average don't adequately account for the risk or (largely unpredictable) consequences of their information being leaked to unintended sources, and rely on trust acquired from repeated interactions with companies, resisting switching costs. When (or if) an especially egregious outcome for consumers is finally recognized after a substantial delay, a large publicly-consumed utility (as in the case of Digg, though potentially services like Facebook in the future) essentially is abruptly eliminated leading to mutually destructive, globally suboptimal outcomes in spite of what neoclassical theory and assumptions would have us believe. Not surprisingly, a society where technology outpaces regulation, legal ambiguities and manipulation all but set up the individuals for failure in properly dealing with exploitative entities. The systematic reinforcement of these inequalities perpetuates the ongoing strained relationships lamented by individual users in the online service market and their continued exploitation.

As a complex, systemic issue, there is no single panacea that, in isolation, will ameliorate this problem. Rather, a successful solution will require attacking the problem from multiple leverage points in tandem and adaptively concerted at different levels (both top-down and bottom-up). For example, given the variability among personal preferences concerning privacy, it is unlikely that blanket policies will suffice for the majority of users, and personalization of information handling is a necessity to capturing the greatest value [91]. As a result, the notion of voluntary disclosure, also referred to as "permission-based marketing," serves a dual purpose in that it can provide a rich source of usable information as well as help build customer trust and brand loyalty. However, market-driven solutions also rely on the accurate/fair valuation of personal information in the public sphere, highlighting the need to simultaneously establish more equitable bargaining levers between the individual and corporate entities. Along the same vein, technological solutions cannot be applied to the recurring problem of user safety in isolation from social solutions, as they will merely lead to technological arms races between parties to covet valued information and security services that are more concerned with profit. With every new advancement in security measures is the means for techniques exploiting system loopholes to coevolve, from the methodical breakdown of DVD Digital Rights Management software in the 90s by the hacking community, to the continuous eruption of new viruses and malicious codes hijacking user accounts, requiring constant updates to elaborate defenses as the next cyber-attack succeeds. Even when the security measures of a large legitimate organization or popular domain are sufficiently advanced to ward off outside attackers for any long period, the corresponding level of clearance and special access protocols demanded by governments has shown potential to open the door to other undesirable intrusions on users.

Perhaps our most interesting result, contrary to conventional wisdom and fairly basic assumptions about rational actors, was the paradoxical way in which individuals were unresponsive to knowledge regarding privacy and dangers and continued to partake in concerning behavior on an ongoing basis. Even with the knowledge and ability to undertake privacy precautions (i.e. awareness of privacy settings), frequently at negligible costs, most individuals choose to continue using default privacy settings. Similarly, people do not generally take extra precautions in online transactions (e.g. don't require extensive assurance of safety from companies) despite a widespread appreciation of the risks involved with information transaction (e.g. of secondary use). In contrast, people are likely to actively resist invasions of their privacy when it violates social norms (for example, the notions of certain privacy invasions violating basic human rights). This suggests that perhaps the best approach to equipping the public against exploitation by companies is not through conventional educational initiatives or informational campaigns, but rather through affinity networks of fellow users and peers asserting the value of one's privacy. Perhaps a larger cultural attitude can ultimately be fostered, regarding actionable, binding privacy terms between individual users

and companies (or appropriate compensation for secondary use) as imperative as the human rights guaranteeing a safe workplace and a living wage for workers.

In spite of the discouraging litany of problems discussed in this paper, the identification of gaps in current knowledge concerning this complex, multi-faceted problem have galvanized further research efforts (especially collaboration between disciplines where problem domains cross over) to address them, some of which are actively underway in concurrent studies. For example, while relatively little information has traditionally been published concerning the perspectives of business executives and formalizing the motivational and incentive pressures that online service provider executives, officers, and company representatives face when dealing with the transmission, storage, and everyday use of sensitive information, recent increased correspondence and collaboration between academic institutions and businesses have created formal channels of such dialogue. In an ongoing expert panel comprised of executives, consultants, and information specialists (among others) intimately familiar with giant information services such as Reputation Defender, the authors of this paper target discussion of these crucial questions, among possible other possible realities of the firm and client interactions not considered by the researchers [96]. Furthermore, on the user psychology front, there exists experimental designs that can more directly observe, manipulate, and simulate transaction behavior preferences of individuals under a variety of hypothetical social conditions and more directly assess perceived value of information than is possible through otherwise passive observations of existing markets. One such study (also involving the current authors) builds on the work of conformity effects and framing in accepting/declining an economic offer, analyzing revealed preferences of college students from a list of hypothetical items saliently related to common online transactions (e.g. the use of a service under explicit terms); Experimental groups are manipulated by ostensible responses of other peers and terms of alternate hypothetical offers, thus aiming to gain further insight into the dynamic effects of salient norms and social reference on human valuation heuristics while controlling for attitudes/beliefs in actual online behaviors [97]. It is our sincere hope that the posterity of this research can inform a comprehensive, multi-pronged approach to addressing these issues of eminently ethical and economic nature, and afford information technology a positive, sustainable role in expanding our economy, helping the public realize value, and truly acting as a tide that raises all ships.

REFERENCES

[1] E. Chan, R. R. Harmon, and H. Demirkan, "Privacy, Value Co-creation, and Service Innovation: Cui Bono?," in *Hawaii International Conference on System Sciences*, 2012, pp. 1–10.

[2] Australian Law Reform Commission, *Protecting Classified and Security Sensitive Information*. Attorney-General's Department, 2004, pp. 1–434.

[3] HIPAA, *Health Insurance Portability and Accountability Act of 1996*. 1996, pp. 1–169.

[4] FTC, "The fair credit reporting act," 2004.

[5] G. L. Bostwick, "A Taxonomy of Privacy: Repose, Sanctuary, and Intimate Decision," *Calif. Law Rev.*, vol. 64, no. 6, pp. 1447–1483, 1976.

[6] D. J. Solove, "A Taxonomy of Privacy," *Univ. PA. Law Rev.*, vol. 154, no. 3, p. 477, 2006.

[7] W. Hartzog, "Promises and Privacy: Promissory Estoppel and Confidential Disclosure in Online Communities," *Temple Law Rev.*, vol. 82, no. Winter, pp. 891–928, 2009.

[8] S. Garfinkel, "Privacy Requires Security, Not Abstinence," *Technol. Rev.*, no. July/August, pp. 64–72, 2009.

[9] A. Ranjbar and M. Maheswaran, "Community-Centric Approaches for Confidentiality Management in Online Systems," in *Proceedings of the 20th International Conference on Computer Communications and Networks*, 2011, pp. 1–6.

[10] R. Westervelt, "The 10 Biggest Data Breaches Of 2013 (So Far)," *Computer Reseller News*, 2013. [Online]. Available: http://www.crn.com/slide-shows/security/240159149/the-10-biggest-data-breaches-of-2013-so-far.htm?pgno=1.

[11] ISO/IEC, "ISO 7498-2:1989, Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture," *Information Processing Systems – Open Systems Interconnection -- Basic Reference Model*. 1989.

[12] C. Crump, "Data retention: privacy, anonymity, and accountability online," *Stanford Law Rev.*, pp. 191–229, 2003.

[13] D. McCullagh, "Feds put heat on Web firms for master encryption keys," *CNET*, 2013.

[14] L. K. Donohue, *The Cost of Counterterrorism*. Cambridge University Press, 2008, p. 512.

[15] J. Menn, "$10m NSA contract with security firm RSA led to encryption 'back door,'" *The Guardian*, pp. 1–5, 2013.

[16] K. Zetter, "RSA Tells Its Developer Customers : Stop Using NSA-Linked Algorithm," *Wired*, p. 3, 2013.

[17] J. Appelbaum, J. Horchert, and C. Stöcker, "Catalog Reveals NSA Has Back Doors for Numerous Devices," *Spiegel Online*, Dec-2013.

[18] S. Worona, "Privacy, Security, and Anonymity: An Evolving Balance," *Educ. Rev.*, no. May/June, pp. 62–63, 2003.

[19] P. Kiecker and D. Pagenkopf, "Confidentiality, Anonymity, Privacy, and Security: Examining Concerns of Online Consumers," 2002.

[20] R. S. Poore, "Anonymity, Privacy, and Trust," *Inf. Syst. Secur.*, no. Fall, pp. 1–5, 1999.

[21] D. Hughes and V. Shmatikov, "Information hiding, anonymity and privacy: a modular approach," *J. Comput. Secur.*, vol. 12, pp. 3–36, 2004.

[22] M. A. Franks, "Criminalizing Revenge Porn: A Quick Guide," 2013.

[23] K. Strater and H. Richter, "Examining privacy and disclosure in a social networking community," in *Symposium On Usable Privacy and Security*, 2007, p. 157.

[24] U. B. Kassebaum, "Interpersonelles Vertrauen: Entwicklung eines Inventars zur Erfassung spezifischer Aspekte des Konstrukts," 2004.

[25] L. A. Cutillo and R. Molva, "Safebook: A Privacy-Preserving Online Social Network Leveraging on Real-Life Trust," *IEEE Communications Magazine*, no. December, pp. 94–101, 2009.

[26] C. Flavián and M. Guinalíu, "Consumer trust, perceived security and privacy policy: Three basic elements of loyalty to a web site," *Ind. Manag. Data Syst.*, vol. 106, no. 5, pp. 601–620, 2006.

[27] J. C. Roca, J. J. García, and J. J. de la Vega, "The importance of perceived trust, security and privacy in online trading systems," *Inf. Manag. Comput. Secur.*, vol. 17, no. 2, pp. 96–113, 2009.

[28] P. McCole, E. Ramsey, and J. Williams, "Trust considerations on attitudes towards online purchasing: The moderating effect of privacy and security concerns," *J. Bus. Res.*, vol. 63, no. 9, pp. 1018–1024, 2010.

[29] Y. Pan and G. M. Zinkhan, "Exploring the impact of online privacy disclosures on consumer trust," *J. Retail.*, vol. 82, no. 4, pp. 331–338, 2006.

[30] S. Lindenberg and L. Steg, "Normative, gain and hedonic goal frames guiding environmental behavior," *J. Soc. Issues*, vol. 63, no. 1, pp. 117–137, 2007.

[31] R. Wagner, "Economic interdependence, bargaining power, and political influence," *Int. Organ.*, vol. 42, no. 3, pp. 461–483, 1988.

[32] A. Dukes, E. Gal-Or, and K. Srinivasan, "Channel bargaining with retailer asymmetry," *J. Mark. Res.*, no. 412, pp. 1–47, 2006.

[33] W. Samuelson, "Bargaining under asymmetric information," *Econom. J. Econom. Soc.*, 1984.

[34] A. Calvo-Armengol, "Bargaining power in communication networks," *Math. Soc. Sci.*, vol. 41, pp. 69–87, 2001.

[35] A. Cleeremans, D. Servan-Schreiber, and J. L. McClelland, "Finite State Automata and Simple Recurrent Networks," *Neural Comput.*, vol. 1, no. 3, pp. 372–381, Sep. 1989.

[36] M. A. Arnold and S. A. Lippman, "Posted prices versus bargaining in markets with asymmetric information," *Econ. Inq.*, vol. XXXVI, no. July, pp. 450–457, 1998.

[37] T. Baldenius, "Intrafirm trade, bargaining power, and specific investments," *Rev. Account. Stud.*, vol. 5, pp. 27–56, 2000.

[38] F. R. Dwyer and O. C. Walker Jr, "Bargaining in an asymmetrical power structure," *J. Mark.*, vol. 45, no. 1, pp. 104–115, 1981.

[39] R. Pritchard, "Equity theory: A review and critique," *Organ. Behav. Hum. Perform.*, vol. 4, no. 2, pp. 176–211, 1969.

[40] E. Walster, E. Berscheid, and G. Walster, "New directions in equity research.," *J. Pers. Soc. Psychol.*, vol. 25, no. 2, pp. 151–176, 1973.

[41] K. Binmore, A. Rubinstein, and A. Wolinsky, "The Nash bargaining solution in economic modelling," *RAND J. Econ.*, 1986.

[42] D. Harnett and L. Cummings, "Bargaining Behavior in an Asymmetric Triad," in *Social Choice (Routledge Revivals)*, 2011, p. 163.

[43] G. Schneider, D. Finke, and S. Bailer, "Bargaining Power in the European Union: An Evaluation of Competing Game-Theoretic Models," *Polit. Stud.*, vol. 58, no. 1, pp. 85–103, Feb. 2010.

[44] S. Dowrick, "Union-oligopoly bargaining," *Econ. J.*, vol. 99, no. 398, pp. 1123–1142, 1989.

[45] A. Acquisti, A. Friedman, and R. Telang, "Is There a Cost to Privacy Breaches? An Event Study," in *International Conference on Information Systems*, 2006.

[46] I.-H. Hann, K.-L. Hui, T. S. Lee, and I. P. L. Png, "Online information privacy: Measuring the cost-benefit trade-off," in *International Conference on Information Systems*, 2002, pp. 1–10.

[47] E. Marandi, E. Little, and T. Hughes, "Innovation and the children of the revolution: Facebook and value co-creation," *Mark. Rev.*, vol. 10, no. 2, pp. 169–183, May 2010.

[48] B. Edvardsson, B. Tronvoll, and T. Gruber, "Expanding understanding of service exchange and value co-creation: a social construction approach," *J. Acad. Mark. Sci.*, 2011.

[49] R. Emerson, "Social exchange theory," *Annu. Rev. Sociol.*, vol. 2, pp. 335–362, 1976.

[50] R. Cropanzano and M. Mitchell, "Social exchange theory: An interdisciplinary review," *J. Manage.*, vol. 31, no. 6, pp. 874–900, Dec. 2005.

[51] P. M. Di Gangi, "The Co-Creation of Value: Exploring Engagement Behaviors in User-Generated Content Websites," 2010.

[52] S. Faja, "Privacy in E-commerce: Understanding User Trade-Offs," *Issues Inf. Syst.*, vol. 6, no. 2, pp. 83–89, 2005.

[53] A. Acquisti and R. Gross, "Imagined communities: Awareness, information sharing, and privacy on the Facebook," in *Privacy Enhancing Technologies*, 2006, pp. 36–58.

[54] B. A. Huberman, E. Adar, and L. R. Fine, "Valuating Privacy," *IEEE Comput. Soc.*, pp. 22–25, 2005.

[55] B. Rao, "Emerging Business Models in Online Commerce," 1999.

[56] M. J. Culnan, "'How Did They Get My Name?': An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use," *MIS Q.*, vol. 17, no. 3, pp. 341–363, 1993.

[57] T. Vila, R. Greenstadt, and D. Molnar, "Why We Can't Be Bothered to Read Privacy Policies: Models of Privacy Economics as a Lemons Market," 2003, pp. 1–24.

[58] M. J. Metzger, "Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce," *J. Comput. Commun.*, vol. 9, no. 4, pp. 1–29, Jun. 2006.

[59] F. Kamari and S. Kamari, "Trust in Electronic Commerce: A New Model for Building Online Trust in B2C," *Eur. J. Bus. Manag.*, vol. 4, no. 10, pp. 125–134, 2012.

[60] I. Ajzen, "The theory of planned behavior," *Organ. Behav. Hum. Decis. Process.*, vol. 50, pp. 179–211, 1991.

[61] A. P. Felt, E. Chin, S. Hanna, D. Song, and D. Wagner, "Android Permissions Demystified," in *Proceedings of the 18th ACM Conference on Computer and Communications Security*, 2011, p. 627.

[62] K. Opsahl, "Facebook's Eroding Privacy Policy: A Timeline," *Electronic Frontier foundation*, p. 4, 2010.

[63] R. Young, "Trust in Facebook Tanking After Privacy Changes," 2010.

[64] A. Wilhelm, "Digg's traffic is collapsing at home and abroad," *The Next Web*, 2010. [Online]. Available: http://thenextweb.com/socialmedia/2010/09/23/diggs-traffic-is-collapsing-at-home-and-abroad/. [Accessed: 26-Jan-2014].

[65] P. Tassi, "Facebook Didn't Kill Digg, Reddit Did," *Forbes*, 2013.

[66] E. Kain, "Reddit Didn't Kill Digg, Digg Killed Digg (Now With Extra Insights!)," *Forbes*, 2013.

[67] P. Berger and N. Nasr, "Customer lifetime value: marketing models and applications," *J. Interact. Mark.*, vol. 12, no. 1, pp. 17–30, 1998.

[68] S. Gupta, D. Hanssens, B. Hardie, W. Kahn, V. Kumar, N. Lin, N. Ravishanker, and S. Sriram, "Modeling Customer Lifetime Value," *J. Serv. Res.*, vol. 9, no. 2, pp. 139–155, Nov. 2006.

[69] E. C. Malthouse and R. C. Blattberg, "Can we predict customer lifetime value?," *J. Interact. Mark.*, vol. 19, no. 1, pp. 2–16, Jan. 2005.

[70] P. M. Senge, *The Fifth Discipline*. 1990.

[71] L. L. Baughman, "Friend Request of Foe? Confirming the Misuse of Internet and Social Networking Sites by Domestic Violence Perpetrators," *Widener Law J.*, vol. 19, pp. 933–967, 2010.

[72] E. P. Kelly and G. S. Erickson, "Legal and privacy issues surrounding customer databases and e-merchant bankruptcies: reflections on Toysmart.com," *Ind. Manag. Data Syst.*, vol. 104, no. 3, pp. 209–217, 2004.

[73] D. Bronski and C. Chen, "FTC vs. Toysmart," *Duke Law …*, 2001.

[74] A.-L. Barabási and R. Albert, "Emergence of scaling in random networks," pp. 1–11, 1999.

[75] D. Singh-Grewal, *Network Power*. London, UK: Yale University Press, 2008.

[76] R. K. Chellappa and R. G. Sin, "Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma," *Inf. Technol. Manag.*, vol. 6, no. 2–3, pp. 181–202, Apr. 2005.

[77] A. Acquisti, "Protecting Privacy with Economics: Economic Incentives for Preventive Technologies in Ubiquitous Computing Environments," in *Workshop on Socially-informed Design of Privacy-enhancing Solutions in Ubiquitous Computing, Ubicomp*, 2002, no. 2000, pp. 1–7.

[78] F. Zhao, *Entrepreneurship and Innovations in E-Business: An Integrative Perspective*. IGI Global, 2006, pp. 1–323.

[79] T. B. Lee, "Entangling the Web," *The New York Times*, pp. 3–4, 2006.

[80] B. Debatin, J. P. Lovejoy, A.-K. Horn, and B. N. Hughes, "Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences," *J. Comput. Commun.*, vol. 15, no. 1, pp. 83–108, 2009.

[81] J. Gideon, L. Cranor, S. Egelman, and A. Acquisti, "Power Strips, Prophylactics, and Privacy, Oh My!," in *Symposium On Usable Privacy and Security*, 2006, pp. 1–13.

[82] J. K. Horowitz and K. E. McConnell, "A review of WTA/WTP studies," *J. Environ. Econ. Manage.*, vol. 44, no. 3, pp. 426–447, 2002.

[83] C. K. Prahalad and V. Ramaswamy, "The Co-Creation Connection," *Strateg. + Bus.*, vol. 2, no. 27, p. 12, 2002.

[84] V. Ramaswamy and F. Gouillart, *The Power of Co-Creation: Build It with Them to Boost Growth, Productivity, and Profits*. New York, New York, USA: Free Press, 2010, p. 288.

[85] N. Hanley and C. L. Spash, "Introduction," in *Cost-Benefit Analysis and the Environment*, 1993, pp. 1–15.

[86] S. Kumar, R. Zafarani, and H. Liu, "Understanding User Migration Patterns in Social Media," in *Proceedings of the 25th AAAI Conference on Artificial Intelligence*, 2011, vol. 1, pp. 1204–1209.

[87] J. Harsanyi, "Measurement of Social Power, Opportunity Costs, and the Theory of Two-Person Bargaining Games," *Behav. Sci.*, no. January, pp. 67–80, 1962.

[88] B. L. Hinton, "The Experimental Extension of Equity Theory to Interpersonal and Group Interaction Situations," *Organ. Behav. Hum. Perform.*, vol. 8, pp. 434–449, 1972.
[89] A. Acquisti and J. Grossklags, "Losses, gains, and hyperbolic discounting: An experimental approach to information security attitudes and behavior," in *Workshop on Economics and Information Security*, 2003, pp. 1–27.
[90] M. J. Lerner and D. T. Miller, "Just world research and the attribution process: Looking back and ahead.," *Psychol. Bull.*, vol. 85, no. 5, pp. 1030–1051, 1978.
[91] M. S. Ackerman, L. F. Cranor, and J. Reagle, "Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences," in *ACM Conference on Electronic Commerce*, 1999, no. 1998, pp. 1–8.
[92] J. E. Boritz, W. G. No, and R. P. Sundarraj, "Internet privacy in e-commerce: framework, review, and opportunities for future research," in *Hawaii International Conference on System Sciences*, 2008, pp. 204–204.
[93] A. F. Westin, "Social and political dimensions of privacy," *J. Soc. Issues*, vol. 59, no. 2, pp. 431–453, 2003.
[94] S. Bauman, F. Newport, L. Rainie, H. Taylor, and A. F. Westin, "Opinion Surveys: What Consumers Have to Say About Information Privacy," U.S. G.P.O. : For sale by the Supt. of Docs., U.S. G.P.O. [Congressional Sales Office], Washington, 2001.
[95] T. Govani and H. Pashley, "Student awareness of the privacy implications when using Facebook," 2005.
[96] P. K. Glazer, "Expert Panel," 2014.
[97] J. R. Straus and P. K. Glazer, "Normative Heuristics," 2014.