

Socially Transmitted Data: The Cost of Convenience and the Value of Defaulting to Privacy

Internet companies' control of data gives them enormous power.
David Parkins, The Economist, May 6, 2017

Information has always been valuable. Data has recently been characterized as more valuable than oil (Parkins, 2017). In the digital age many companies are focused on the need to gather any and all data for short term benefits without regard to the long-term risks. Exchanges of information online are becoming seamless, frictionless, and extremely convenient for consumers, giving marketers and databrokers increased ability to collect and analyze data. Responsible collection and use of data is valuable, but is there value in NOT collecting information? This overview of a journal article¹ addresses the nature and evolution of privacy and security and posits that **defaulting to privacy** and allowing individuals to provide the information they actively decide to provide is more valuable than the current system of collect-information-now and figure-out-the-value later. It also proposes the use of a matrix to help consumers characterize and navigate the difference between trusting companies and simply having faith.

Knowing when, where, and how their information is collected, stored, and disseminated: Does it matter?

Understanding the details and technology behind online individual information exchanges is perplexing to the lay person. Individuals are confronted with complexity and context challenges because most individuals in the digital age cannot and do not pay attention for lengthy periods of time. They are overloaded with information and often find themselves agreeing to terms and policies without understanding the details (frequently not even reading them). This difficulty puts individuals at risk. It makes them vulnerable when making decisions quickly online. The convenience provided by technology is costly and instead of benefitting exchanges, transparency adds to this cost by providing more information for individuals to wade through. As Herbert Simon expressed in 1971, "A wealth of information creates a poverty of attention." This lack of attention, or Continuous Partial Attention (Stone, 2007) is only exacerbated when individuals are making decisions as cognitive misers (Fiske and Taylor, 1991) and having to narrow the information used in decisions. The quality of data is also an issue, increasingly forcing people to attempt to determine the authenticity of information. Free exchanges of information come with costs and more data is not a sufficient solution. In addition, employing algorithms to filter information may intend to help, but the lack of transparency or oversight for these proprietary systems poses problems. This is becoming evident and especially troubling with the potential to weaponize data.

Socially Transmitted Data: Negative Externalities

As people exchange more information with apps, platforms, companies, and each other, their information spreads online farther than they may understand – as socially transmitted data (Walker, 2016). Much like a virus, these technology STDs often spread quickly and unbeknownst to the individual. Privacy policies or terms and conditions explicitly state that the information may be shared with third parties, affiliates, partners, etcetera but it is rare for individuals to read these lengthy documents of legalese. The Federal Trade Commission has encouraged making these clearer and understandable, yet even with clarity the reality is that people's information is collected, stored, and disseminated, often with an unlimited number of other users for many

¹ Walker, K. L. (2016). Surrendering information through the looking glass: Transparency, trust, and protection. *Journal of*

purposes, expected and otherwise. Users have little to no control of that information or versions of the data after the initial exchange. There is also no incentive (or cost) to business unless the transmission of the data cause explicit harm and that harm is discovered and reported. And that cost is contingent and so far downstream that the actors are typically unconcerned. Because users do not even understand what they are giving up, they are unable to perceive, let alone mitigate, the long term risks of the exchange. Companies often have no incentive (other than ethics and/or punishment) to internalize any socially responsible actions with the spread of data, thus increasing the vulnerability of the data, the potential for unintended consequences, and negative externalities.

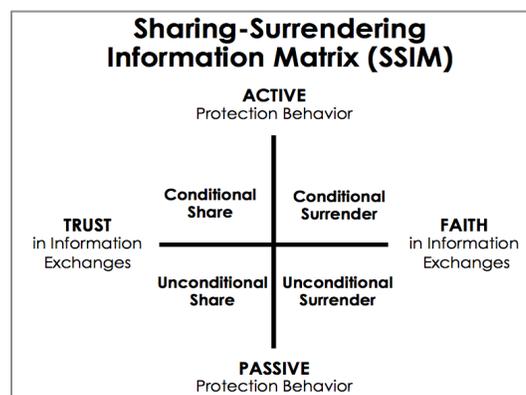
Certainty and Protection Behavior: Characterizing Risks in Exchanges

The sharing-surrendering information matrix (SSIM) outlines two key constructs to help individuals and companies characterize information exchanges.

1. **Level of certainty with information exchanges.** Certainty in an online information exchange allows the user to **trust** in the exchange. Uncertainty leads the user to only have **faith** in the exchange. These are important distinctions for risk assessment.
2. **Conditions place on information exchanges.** It is also important to help individuals distinguish between levels of protection in their information exchanges. Classifying active or passive protection strategies as placing **conditions** in the exchange helps individuals understand the subtlety of protection, or for some groups clarifies that ‘public versus private’ access controls may not be adequate protection.

Since trust and faith differ depending on the level of certainty, the issues involved with accuracy of data and knowledge of which parties are involved in the exchange are more easily characterized for individuals and firms. While companies struggle to increase trust and enhance transparency, for most consumers this is not useful without categorization. When are they trusting and in which exchanges are they simply having faith in their information exchanges? How much should they protect themselves and what types of privacy settings equate as active protection? Portraying these constructs is essential for clarifying the risks involved with increased reliance on technology and desire for convenience. Thus the SSIM portrays when people exhibit trust in an exchange they are **sharing information**, whereas when they exhibit faith in an exchange they are **surrendering information**. These constructs are depicted in a 2x2 matrix, allowing marketers and policymakers a tool to help consumers characterize risk in their information exchanges (see Figure 1).

Figure 1.



Source: Walker, 2016, p. 149 (reprinted in Andrews, J. C., & Shimp, T. A. (2017). *Advertising, promotion, and other aspects of integrated marketing communications*. Nelson Education.



Defaulting to Privacy: Value in Accuracy

Information may be power, but inaccurate information causes inestimable damages (e.g. weaponization of data). As stated, defaulting to privacy allows individuals to provide the information they choose to give. This helps, since the nature of online information exchanges in the U.S. is encouraged by concepts of openness, transparency, and trust. There are varying views of information exchanges in an innovative and technology-integrated society, from utopian to dystopian. Yet these views are extremes on a continuum that obviously involves risks and benefits. These risks and benefits are exacerbated when information is not verified. Accurate information about individuals is more likely to be quality information and allows for both parties in an exchange to benefit. Defaulting to privacy is a realistic solution with the technological advances and tools that now exist. Companies should realize that if they know a consumer only wants to provide some information or certain data about themselves, then that knowledge in and of itself is valuable. Creating a tool for consumers to have control over the information they provide would be empowering. It would satisfy regulatory and self-regulatory concerns and reduce the costs involved with errors in analysis based on inaccuracies.

Self-regulatory efforts and government regulatory efforts would benefit from defaulting to privacy. Note that defaulting differs from permission in the sense that users are not consenting to data being used, but instead giving companies information and choosing *which data they want to exchange*, improving accuracy and the value of the data (in the short and long-run). Defaulting to privacy means utilizing technology and algorithms to help users decide and determine which of their valuable data they prefer to exchange. The details of the actual information exchange(s) are important because they are so diffuse and infinite. Assuming information needs to be exchanged is lazy. People are unable to understand the nature of the exchange at the onset of the exchange - what are they giving up, how will the information be used, and how can limits be placed on the exchange. Therefore defaulting to privacy empowers the current solutions of transparency and trust. This also addresses many issues about youth and privacy.

I hope our wisdom will grow with our power and teach us that the less we use our power the greater it will be.
Thomas Jefferson

Decreasing Risk by Increasing Awareness

The goal of the SSIM is to increase the awareness for individuals and firms about the realities involved with their information exchanges. Characterizing the level of certainty in the exchange (trust or faith) and distinguishing between the amount of protection involved (active or passive) allows individuals to understand whether they are sharing or surrendering information, conditionally or unconditionally. This tool, alongside a move to utilize technology and default to privacy will help to empower consumers and benefit firms by **encouraging authentic trust and relevant transparency for convenient yet controlled access** in information exchanges. Increasing awareness also involves education. This material will be presented by the author at a training session for the California Legislative Staff about socially transmitted data and the blurring lines between professional and personal exchanges of information online (social media in particular). It is also the focus of a Town Hall event for the California LegisSchool Project Town Hall in February 2018, *Social Media: Friend or Foe?*²

² The LegiSchool Project is a civic education collaboration between California State University, Sacramento, and the California State Legislature, administered by the Center for California Studies. The Project's mission is to engage young people in matters of public policy and state government by creating opportunities for students and state leaders to meet and share ideas on the problems affecting Californians.
http://www.csus.edu/calst/legischool_project/