Finding Balance in the Future of Technology:
An Analysis of the Dichotomy of Freedom
p101 (2158 words) (pr)

Danny Yu
Jonathan Hong
November 14, 2011

Few ideas are as prevalent and stalwartly supported in the world of modern democracy as compromise. Compromise is touted as the lubricant necessary for smooth operation of democratic society. Yet, following this mindset has allowed what David Brin calls "devil's dichotomies" to develop (320). These false dichotomies often involve the balance or sacrifice of two essential virtues, forcing those who believe in them to sacrifice something they cannot do without. Throughout his book, *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?*, Brin posits that freedom, in this case meaning the flow of information need not come at the cost of privacy, a word that comes to mean the ability to control the flow of information regarding anything that has to do with you. While privacy is constantly being redefined(as shown later in this paper), this is the generally accepted definition at this moment in time. While modern technology has brought about the ability to collectively share information with a huge number of people in a short amount of time, perhaps against your own will, it can also be used to promote privacy, both of which have profound impacts on our ever-changing society.

Examples of technology enabling easy, unsolicited observation of personal activities and habits are already well in play. In offices, credit bureaus and even your own home there are a plethora of technologies widely available for monitoring your habits and activities (Brin,56). These range from keyloggers and cameras to databases of personal information collected by various agencies, sometimes with your consent, that bar you access to the information that they've collected on you. Not all these entities are allowed free will however. The fourth amendment, though filled with loopholes, has been interpreted and upheld as an imperative to maintain personal privacy (Brin,71). That the fourth amendment only protects individuals from invasions of privacy instigated by the state is among the many limitations of the reach of the fourth amendment. Nevertheless, it has set a precedent for privacy, protecting an individual's "right to be let alone," to be free of "unreasonable interference" and to be protected from overdue harm (Brin, 74).

Along with examples of technology that are enable the ability to be observed easily, Brin poses these hypothetical scenarios throughout his book, some of which are chillingly accurate descriptions of recent events. He mentions that "airport security might be a potential application if [technology allowing nude imaging] is introduced," a notion which has actually been realized (Brin, 62). Brin also notes that the concept of small, remote-controlled cameras is already well on its way to actualization, as a number of technologies necessary to create such a thing are

already in existence - and this book was written in 1998. That a technology exists does not mean that it will necessarily become pervasive throughout a society. The Transportation Security Administration (TSA) had, as of the time of writing this, recently foregone the invasive imaging scanners, instead replacing the images with generic models that simply reports anomalies on a person and their relative positions on the body (Stanley).

While we have just discussed technologies which support freedom and policies which inhibit it, the relationship is by no mean unilateral. There are a number of technologies which promote privacy and concealment, despite policies which would support freedom and openness. Anonymizers, a general term which refers to technologies that work to conceal senders and recipients of electronic messages, are one such example. These can come in the form of remailer services, which allow the sending of e-mail messages via a third party e-mail service, which can only be traced back to the actual sender by the service (pg. ?). Encryption technology also works to conceal, by disallowing anyone but the receiver or sender of a message to view its contents, although such technologies do not typically work to conceal the sender or recipient's identities (pg. 280).

Likewise, there have been a number of policies and systems of distribution that were intended to promote the freedom of information by rewarding innovators for sharing their creations. Intellectual property (IP) laws were, in fact, originally designed for just this purpose. Patents allowed for the widespread use of new technologies in exchange for commission and royalties. Not only did patents promote sharing with others, but they also promoted using the latest technologies as they arrived, benefiting society as a whole. Recent trends have shifted the use of patents to promote, instead, the staunching of new innovations by refusing to grant licenses for patent use or to offer them only at ostensible royalty rates (pg. 94). Some of the fear regarding the promotion of information comes from the lost profits of content distributors, who "worry about the new era ahead" (pg.96). As the dissemination of the information they provide directly relates to lost profits, they are among the most ardent supporters of information control, pushing for legislation such as the National information Infrastructure Copyright Act.

Freedom, while often seen as having intrinsic value, also serves to fulfill pragmatic concerns as well. This is accomplished through a cycle of critique, accountability and improvement. Brin describes one example of the principle put to good use in the case of Experian, which "predicted chaos" should their customers ever be allowed to view their own information, but instead experienced "increased accountability, accuracy, and efficiency" (pg. 59). How would this be accomplished in a transparent society? Brin posits that vigilant watchers, which he compares to T-cells, would scrutinize every major power, pointing out its errors and holding them up for criticism (pg. 142). While such a system would not be perfect at first, Brin holds that with time such a system of checks and improvements would itself improve, leading the world closer to an error-free society. As Brin puts it: "Humans have found one fairly reliable antidote to error: criticism" (pg. 134).

The concept of "Tag commentary" that Brin devises as a means of judging the quality of content in the new age bears some consideration. Brin poses that such a system would render

propaganda ineffective, by mere means of providing instant access to responses and opinions of others on a piece of content's trustworthiness (pg. 260). This could be accomplished by either direct links to other content reviewing the merits prior or by even a simple "thumbs up or thumbs down" system that keeps a record of how many people viewed the content positively or negatively. If this sounds familiar, then it is most likely because such a system is already in place on various media sharing websites, namely, YouTube. As many can likely attest, this does not eliminate the problem of worthless content, but does serve to alleviate it somewhat. On the other end of the spectrum are memes, defined as "self-replicating ideas," which propagate without any active effort. It is a word many are likely familiar with, which some of us may find synonymous with outright tomfoolery, and clear evidence that ratings systems, such as the the derision of net denizens, is not fool proof. It may only be a matter of time before technology finds a technical solution to the problem, however.

Much of this paper has discussed how policy and technology promoting or demoting freedom might impact society, but not much has been written on how, exactly, freedom can help to preserve privacy. Brin asserts that the choice between freedom and chaos versus order and tyranny "arises more out of sour romanticism than any reasonable argument" (Brin, 204). He goes on to write that many of the criminals who commit destructive, illegal activities do so mainly because they have little fear of being caught, and as a result, are largely undeterred from committing crimes, including voyeurism. If surveillance technology were universalized, than few people would choose to pry into others' private affairs without good reason because of the likely chance that someone else would notice that they were peeping, much in the same way people would be unwilling to ogle others at a restaurant due to the high chances of them being caught (Brin,14). Rather, to truly safeguard privacy necessitates not the erection of barriers, but the tearing of them down, for the former will, in the long run, only cause an irreversible state of affairs in which the public is so underpowered and outclassed that they will never again know true privacy (Brin, 209).

Despite all this talk surrounding the issues of privacy, one pervasive question looms ominously overhead: what is privacy? According to Brin, privacy has actually been quite hard to define, as many legal authorities have debated it without any clear resolution (Brin, 70). He does, however, bring up Dean William Prosser's analysis of privacy, written in 1960, which states four categories of privacy torts, or lawfully wrong breaches in privacy. These include the tort of intrusion, disclosure of offensive and publicly irrelevant facts, false light, which is akin to slander and appropriation, which includes misconduct facilitated by private information, such as identity theft (pg. 72). While these torts provide a useful structure for defining privacy legally, few would argue that their privacy has not been breached solely on the basis that none of these torts have been committed. Yet, privacy is a relative novelty. In addition to the restaurant example discussed earlier, which describes the present state of privacy, past privacy was largely an obscure notion as few people could really be guaranteed such a thing (Brin, 68). In smaller communities, any misconduct or ill-spoken words were quickly known by everyone, with little

recourse for anyone but the rich (Brin, 216). In essence, privacy is known best by those with the least interesting lives (pg. ?).

Let us now consider that the ideas posited by Brin are indeed all correct. Would it be reasonable to assume that civilization will take the next logical step and tear down the entire infrastructure of technologies promoting privacy? Not likely. In the case of governments and corporations, they would hold onto their power in large part by their loathsome distaste for relegating power to others, especially when it could be used against them (pg. ?). There have been many exceptions throughout history, perhaps none more relevant than the creation and widespread adoption of the internet, which was intentionally designed for robustness (Brin, 37). As for how a common individual may attempt to gain power equal to the already powerful, encryption has been posed as the tool of choice by many technological aficionados, such as Hal Finney, who believes that "encryption offers for the first time a chance to put the little guy more on an even footing with the big powers of the world" (Brin,273). Why would somebody given the choice to force someone else to be held accountable or to erect walls around oneself choose the latter? One possibility is simply that people have less fear over situations that they are more in direct control of, regardless of the actual level of threat present (Brin,156). In essence, to create a transparent world is so controversial and so difficult to enact that in order for it to even become plausible, it would have be agreed on by nearly a consensus of the world's population (pg. 320). As Brin puts it, "whenever a conflict arises between privacy and accountability, people demand the former for themselves and the latter for everybody else" (Brin, 12).

Privacy, at least in the short term, has its applications however (pg. ?). In the case of military action, an inability to conceal the location of a strike or ambush would cripple a smaller faction's combat capabilities over a superpower. In addition, conservation and protection of sites, areas or individuals would be made very difficult if their locations were constantly being broadcast around the globe (pg. ?). For many of us, however, such things are of little concern, as they have little effect on our lives. While privacy is still wholly possible in a world of increasingly more powerful tools of surveillance, that does not mean we should forgo the simple question of whether or not we should care if someone sees what we are doing (pg. 250). It stands to reason that someone with nothing to hide cannot be caught. Of course, no ideas are without fault, and even this very paper which is intended merely to analyze the ideas presented by a larger work is wholly fallible. Thus, I shall end with the words that Brin's book arguably promotes as much as it does its subtitle: "I could be mistaken" (Brin, 294).

References:

Brin, David. *The Transparent Society: Will Technology Force Us to Choose between Privacy and Freedom?* Reading, MA: Addison-Wesley, 1998. Print.

Stanley, Jay. "TSA Scanners Start Moving From Naked Bodies to Stick-Figure Outlines." Web log post. *Blog of Rights*. American Civil Liberties Union, 20 July 2011. Web. 14 Nov. 2011. <http://www.aclu.org/blog/national-security-technology-and-liberty/tsa-scanners-start-moving-naked-bodies-stick-figure>.