U.S.S. Privacy

Cardboard and duct tape. Yes, cardboard and duct tape are currently holding my life in their hands. Unfortunately, neither of them is known for having particularly strong hands. Or any hands at all. Thus, my predicament at the moment is likely not anyone's ideal. A corrugated cardboard box, which once held the 27-inch Samsung television now sitting on my bedroom dresser, is my punctured raft. Silver duct tape, which had lain tainted by dust in an ancient toolbox until about a month ago, is plugging my flotation device's holes. I wish I meant "cardboard," "duct tape," or "punctured raft" metaphorically; regrettably though, none of them is figurative language. My homemade cardboard boat, held together only by duct tape and the desperate hope of an amateur captain, is sinking.

There is a name for this traumatizing experience. In fact, it is a celebrated event ironically called the Howard County Boat Float. The rules of the Boat Float state that participants can use only cardboard and duct tape for constructing their aqua vehicles. Based on my one-man ship's result, I am not quite a master of the materials yet. Most disastrously, I did not gain this insight before race day. I simultaneously bail water with cupped hands and contemplate how to MacGyver my way out of this one. As I become wetter and wetter, and my boat becomes soggier and soggier, I arrive at a decision. I only know what I already know. Thus, I will use what I have already used. I will simply use more of it. I reached underwater for the roll of soaked duct tape at the bottom of my box, and I began patching duct tape with more duct tape as water continued to pour in and drench me.

Just like my television-box raft, the vessel of modern privacy is urgently close to sinking. As in Sebastian Junger's novel, the perfect storm of technology hit when rapid processing power and enormous data storage capability combined with the Internet, leaving the helpless boat of contemporary privacy capsized in their wake.

Albert Einstein defined insanity as "doing the same thing over and over again and expecting different results" ("Quotations"). Trying to fix a problem with more of the problem, as I tried at the Boat Float, is one interpretation of his point. Grievously, the Internet's commercial industries have taken this exact route in trying to turn the privacy boat right side up again. Their material of choice is not duct tape, however. Their "solution to the overabundance of information," which is the result of no data being private anymore, "is more information," or less privacy (Weinberger 13). In order to the insanity of it all, one first needs to fully comprehend the current upside down state of privacy.

The only aspect of the amorphous concept of privacy that scholars tend to agree on is the following: privacy consists of several interrelated aspects. Technology, though, has distinguished a single one of privacy's aspects as the most relevant. That aspect is control over the flow of information. It is the most pertinent today because the Internet and computers enable the permanent storage and instant transfer of incredible amounts of data. Acxiom, Amazon, Google, and Facebook have been the most prominent when it comes to using this ability to obtain and utilize individual's information. This paper will argue that the resulting transparency provides an equal distribution of advantages and disadvantages for today's society. Then, in conclusion, it will suggest that both legislatures and individuals adapt their current perspectives on privacy because there is no returning to the "old information lock-down" (Abelson).

It is problematic that a concept as prevalent as privacy has never had a precise and transparent definition. Neither its scope nor even its classification is very lucid. While some scholars insist that privacy is simply a derivative of a more explicit right, other scholars argue that privacy is its own right. If it is its own right, there is still further debate over whether it is a moral fundamental or a constitutional justice (Magi 189).

Nevertheless, most scholars can agree on one fact about privacy. It is multifaceted. The

amorphous concept can be defined as the privilege of solitude and personal space, the freedom from interference and observation, and the protection of one's individuality and one's intimate relationships (Magi 189; Ramsay 289, 290). It has also been considered synonymous with secrecy, autonomy, and liberty (Tavani 5, 9). By far the most relevant definition of privacy today, though, is having control over one's personal information (Ramsay 288). Its importance exists in the fact that individuals no longer have said control in contemporary society, because technology swiped it away from them.

Because privacy is a network of interrelated ideas, it is only appropriate that the most expansive network of interrelated ideas ever be its downfall. When the Internet arrived--along with exponential growth in data storage, processing power, and communication ability--it impacted the already shaky foundation of privacy like an earthquake (Abelson). The tremors demolished every preconceived notion regarding personal information, but fresh realizations took their places as soon as the shaking came to a halt. With the advancements in storage, the personal information of every person in a nation can fit on a laptop (Abelson). Simultaneously, the increase in processing power enables computers to sift through all of this data in only moments. Finally, because of the global network that is the Internet, all of the analyzed information can be transferred anywhere instantly.

Technology is such a necessity nowadays that some might say it could fit in Maslow's Hierarchy of Needs, perhaps after safety but before love and belonging. Consequently, its utilization is inevitable. As people use technology, they betray their privacies in two distinguished ways: "digital footprints" and "digital fingerprints" (Abelson). "Digital footprints" are traces that users leave behind with full knowledge that they are doing so. An example is the input of one's name and address when making an Amazon purchase. "Digital fingerprints," on the other hand, are invisible. One "digital fingerprint" is a user's IP address. Sites collect this

unique number from every one of its visitors. Another "fingerprint" is left because most domains nowadays leave cookies on the computer, which will transfer information back to their creators even after visitors have left their page. In the PC era of 1985 before the Internet, everything done on the Internet seemed ephemeral (Batelle 10). "Digital footprints" and "fingerprints," however, make everything quite permanent. "The problem is not just the existence of digital fingerprints, but that no one told us we are creating them" (Abelson).

Given that every user on the Internet is leaving behind these trails, someone must be following them all. As a matter of fact, quite a few groups are playing detective. Almost every commercial company in contemporary society tracks users, but it initially began with just a few. Moreover, it commenced years before the popularization of the web and, more significantly, before anyone had any idea that data collection existed. Beginning in the 1990s, data aggregators, which had been around since the 40s, gained momentum as computers continued to adhere to Moore's Law. Moore's Law simply states that the processing power of computers doubles approximately every two years.

The largest of these data mining companies at the time was Acxiom (O'Harrow 37). Acxiom's business was in collecting data fragments and analyzing them for relevancy. Acxiom then sold its statistics to companies in the credit card, insurance, and other industries (O'Harrow 37). For reference, the web took off in 2003. Until then, Acxiom accumulated much of its data via the telephone; however, most individuals had no idea their information was being preserved and sold (O'Harrow 52). Acxiom has since migrated to the Internet for data aggregating, which is also the medium of the other major companies involved. Currently, Acxiom has an average of 1,500 pieces of data about each of the 96% of Americans whom it has targeted (Pariser 42, 7).

Amazon was another primary pioneer as the data market expanded. Amazon launched at the very beginning of the dot-com bubble in 1995 but was one of the few Internet companies to

come out alive after the burst. Amazon's business strategy revolved around selling books online in a manner that reflected buying books personally at a local bookstore (Pariser 28). To accomplish such a feat, Amazon observed its customers purchase histories so that it could predict their future investments. Though it may have seemed like an invasion of privacy, such concerns were forgotten by Amazon when the design reaped profits and by customers when they received recommendations. Despite intentions, this approach was more foresight than reminiscence. Amazon's key of personalization became the skeleton key for the success of all future online businesses.

A third principal pilot of the online data collection business was Google. When it launched in 1998, Google was not the first search engine. Because of the overflow information on the web, search engines inhabited the net rather quickly. Google's creators, however, devised a page ranking system that was undoubtedly going to make it the preeminent one. Academic papers gain more credibility every time future papers refer back to them. Google operated in a similar fashion, by judging the authenticity of a web page off how many times it is linked to from other sites (Pariser 32).

As Internet users experienced Google's efficacy, this particular search engine became integral for navigating the web. Stealthily behind the search bar though, Google was recording every query and every result ever entered. Inside the black ops, it became clear that with this search history, "Google had more than its finger on the pulse of our culture, it was directly jacked into the culture's nervous system" (Batelle 2). This "Database of Intentions," which Google is still creating, may be the most accurate representation of a culture in history (Batelle 6).

Google perceived that the foremost results for one person were not the foremost results for another person. In order to continue giving better results, the search company steered in a

direction similar to Amazon by incorporating personalization. Google then introduced Gmail, which was the first in a steady line of products, which gathered more personal information about users than simply their search histories provided.

How much extra information is Gmail providing Google? Google's Gmail, like all email hosted on individual servers, has the right to keep copies and analyze its members' mail. "It's a bit like letting the post office keep a copy of every letter you send, but we are so used to it, we don't even think about it" (Abelson). Google's future products like Google Earth and Google Buzz have been even more intrusive but are also even more innovative. For the twenty-first century individual, the sacrifice is worth it.

Finally, one of the more recent pioneers in online data collection is Facebook. Whereas Google uses the charades and masquerades of inventive products to conceal its true purpose of data aggregation, Facebook transparently asks its users to provide said data. Facebook's product is a network of personal information. The information is entertainment for the customer, but it is profit for Facebook. In 2009, the site reached 300 million members and made expansions that drastically decreased privacy even further. Facebook adopted omnipresence and began directly collecting data from any other sites on the web that chose to affiliate themselves with the social media giant (Pariser 39, 40). Resultantly, Facebook members' data seems to be in everyone's control but their own.

Because of the computer, the Internet, and other technologies, data aggregation has become an extremely profitable industry; hence, companies like Acxiom, Amazon, Google, and Facebook now control everyone's information. While this truth may seem absolutely appalling, it has both advantages and disadvantage, which will follow. Additionally, the modern laws on privacy will reveal themselves to be inadequate. Consequently, both governments and individuals need to step back and decide which parts of privacy's many are the most valuable

and realistic today.

The aforementioned intrusions of privacy would have, a decade ago, seemed overwhelmingly revolting. Currently though, society either does not know about, does not care about, or feels powerless in avoiding such intrusions (Abelson; Batelle 15; O'Harrow 62). According to studies, the majority of Internet users fall into the second category, meaning they likely have a partial understanding of the Internet's effects on privacy, but they are not worried about it (Abelson). The following question remains: why are they not? The many answers lie in the many benefits of having no privacy.

Several benefits for the individual accompany a society with lesser emphasis on privacy and a greater emphasis on transparency. The most obvious positives are also the most superficial. For example, customers save both time and money when companies store their personal information. Individuals do not experience the frustration of redundancy when a website saves their passwords and does not make them type the codes in every time (Abelson). Also, consumers are willing to sacrifice sharing their purchase history with Amazon if it translates to occasional discounts. Another example of an extravagant benefit is convenience. While encrypted email sites, which do not analyze and save their members' mail, do exist, most Internet users choose Gmail, Yahoo, or another unencrypted private server for their electronic communication because of naught but convenience (Abelson). A final superficial positive is that exposing oneself and forgetting privacy is thrilling. It always has been to the narcissistic human race; however, only recently have the moments of forgetting become unforgettable (Abelson).

The operating system Linux, the web browser Firefox, and the online encyclopedia Wikipedia imply one of transparency's most influential positives. The common thread among all three of these technological projects is that they are open. Open, in their cases, means that everyone has permission to modify them, as long as the modifications are made available to the

public for free. This large-scale collaboration is creating a new "collaboration economy" (Tapscott 31, 32). In the "collaboration economy," more innovation is possible than ever before because the development team of a project knows no bounds (Tapscott 32). Furthermore, because all of the products and information are completely transparent, everyone benefits.

Even the commercial naysayers, themselves, recognize the benefits of this free-flowing information. However, they fear that it will discourage innovation and production in businesses because the entire Internet can pool together to make products equivalent to their commercial counterparts. Thus, these critics proclaim that mass collaboration and its transparency eliminate room for earning revenue (Tapscott 17). Quite the opposite is true, though. Businesses will be encouraged to innovate even more creatively in a manner only possible because of their monetary resources; hence, they can still be competitive and profitable. Individuals as well benefit because the "collaboration economy," which is only made possible because all information now is either voluntarily or involuntarily non-private, forces companies to be more transparent and global if they have any intent of success (Tapscott 22, 31). Consequently, the businesses are forced to have only as much privacy as individuals.

Though the preceding benefits of no privacy are enough to make some people discard concern about "digital footprints" and "fingerprints," its drawbacks make it harder for others to forget so easily (Abelson). The first negative is actually a result of the skeleton key that Amazon molded back in 1995. The Internet's content is virtually endless. Amazon's merchandise recommendations, Google's personalized results, and Facebook's censored news feeds are each company's attempt to guide the user through all of the web's information. Based on users' preferences in the past, the companies predict what each one wants to see in the future. The negative result is that users are limited from discovering new interests and learning about fresh perspectives. As Google expert Siva Vaidhyanthan notes, "Learning is by definition an

encounter with what you don't know, what you haven't thought of, what you couldn't conceive. … The kind of filter that Google interposes … shields the searcher from such radical encounters" (Pariser 91). This content restriction is known as the "filter bubble," and though its intentions are legitimate, its results in practice are inhibiting (Pariser 15). In other words, "I only know what I already know."

A lack of privacy is also responsible for negatively impacting identity. "When it comes to identity, getting things almost right just doesn't work. We care too much about it for that. … Identity is about belonging and connectedness and culture" (Shroff 302-303). "Connectedness" is an appropriate word here for contemporary identity, because identity has turned into how we connect to others more than how we view ourselves (Tancer 3). Privacy is the only concept fit to play certain roles in society. Thus when privacy is not there to fill its roles, social connections are hindered. One of its positions is in preventing the overextension of social interactions. Privacy enables individuals to reveal only the parts of themselves suitable given the audience. This concealment disallows any one group from exercising too much control over an individual (Abelson; Magi 14). Because privacy has disappeared, data aggregators have gained such control. As a result, they allow our identities to be immortalized and scrutinized on command (Batelle 14).

While too much transparency in personal relationships results in a loss of identity, a lack of privacy in a bureaucracy results in an imbalance of power between the government and its citizens. The final cost of losing privacy is the following: when individuals lose a space for voicing minority views or organizing resistance, bureaucracies gain too much power (Magi 18). Active resistance movements, however, in this privacy-free society have proven quite the opposite. The human-rights activist website WikiLeaks regularly releases confidential government documents to the public. In late 2010, the site published more than 250,000 U.S.

diplomatic cables, which gave an unfiltered look into bureaucracy. Furthermore, the recent revolts in the Middle East against unpopular regimes were largely organized via public social media sites. Though current events prove that a lack of privacy does not directly translate to an imbalance of power in bureaucracies, government and privacy do have a bit of work to do on their unsteady relationship.

Because the positives of not having privacy have just as much of a case as the negatives, privacy in the legal sense is still in development. "Modern privacy law is often expensive, bureaucratic, burdensome, and offers surprisingly little protection for privacy … The U.S. is not lacking in privacy laws. But privacy has been legislated inconsistently and confusingly, and in terms dependent on technology contingencies" (Abelson). One exemplary discrepancy caused by early privacy legislation originates in the Fourth Amendment. The Fourth Amendment prohibits unlawful searches and seizures whenever privacy can be reasonably expected. However, because technology has radically reduced privacy, the concept that is supposed to protect citizens is now backfiring on them as it fails to forbid more and more searches and seizures (Ku 876).

The Privacy Act of 1974 also illustrates inadequate U.S. legislation. It established guidelines for the timing and method of governmental data collection that limited the government's power of privacy violation. After 9/11, however, Acxiom offered its services to the government for the purpose of countering terrorism. It was then that the government recognized a rather significant loophole in the Privacy Act. It regulated data aggregation by the government but not private data aggregation (Abelson; O'Harrow 57). Further, one of the Patriot Act's effects actually makes any data collaboration of this type with private aggregators completely secret.

The current U.S. policies are equally ineffective when it comes to legislation that is

supposed to moderate Internet companies rather than the government. The Electronic Communications Privacy Act of 1986 forbade Internet Service Providers from tracking their users' emails. The email services that most people use today, however, run on private servers, which the act does not regulate at all (Batelle 11). Another representation is the Video Privacy Protection Act of 1988, which made it illegal for video stores to keep records of its customers' rentals for any extended period of time. Twenty years later, Amazon's business revolves around keeping records of just that type (Abelson).

Forgetting the incompetence of U.S. laws, what truly puts legislation of privacy on the Internet out of reach is the fact that the Internet is worldwide. Any one government's laws do not clearly apply to other countries' citizens. Moreover, while the U.S. basically lacks any standard privacy policy to which companies must abide, the European Union sets mandates that closely resemble the Fair Information Practice Principles of openness, disclosure, secondary use, correction and security. In reality, though, the EU's policies have not been much more effective than the U.S.'s. One significant contributor to this truth is that "the unlawfulness of any action does not explicitly prevent it from occurring, suggesting only that it be avoided" (Matthew 42). Information compilers often ignore laws because they are too weak or too obstructive (O'Harrow 39). Consumers also disregard laws that are not in accordance with their desires. The entertainment industry provides a prime paradigm here because consumers have perpetually neglected all laws against move and music piracy (Matthew 43).

Nevertheless, the U.S. and other nations ought to at least attempt more effective legislation. Governments need to found their regulations on privacy's previously discussed advantages and disadvantages (Abelson). Personal information is now permanently public, because data aggregators have collected, analyzed, and shared it irreversibly. Individuals have lost the control, and it is impossible for them to regain it (O'Harrow 66). Consequently, future

legislation must abandon the idea of trying to limit who has access to information. Instead it needs to focus on restricting the inappropriate use of said information by those who now have control (Abelson). Like the governments, individual citizens are going to need to adapt as well.

Thus individuals ought to adjust how they value privacy because certain aspects of it have become decidedly extinct. Instead of valuing the control over information, people must try to find value in solitude and domesticity. Solitude provides a time of reflection and a time to genuinely accept oneself. Domesticity provides a feeling of security and a place for experimentation inside the home and with family (Ramsay 290, 291). Both of these aspects remain attainable in the twenty-first century. Most importantly, though, everyone must learn to place value on "the maintenance of a sphere of inviolability around each person" (Ramsay 291). Though businesses collect personal data for their profit and governments set up surveillance to protect national security, it is fundamental that every individual is still treated with the dignity and respect of a human being.

Cardboard and duct tape. As I layered more duct tape on top of the existing pieces, my cardboard boat gradually stopped gaining water and eventually retained a constant level. The corrugated raft, and I, would live above water for at least another day. It was clear to me, though, that if I wanted to sail the Boat Float course again, I was not going to be able to do so in a raft that was repaired by such an insane method. The repairs were ephemeral, but they needed to be permanent. The repairs needed to be as permanent as information on the Internet.

The perfect storm of technology has further obscured the already amorphous concept of privacy. Because of the advantages of maintaining privacy, many individuals aim to right the capsized boat, while others have already abandoned ship for the benefits that come with the new vessel named transparency. In order to weather the tempest, though, each individual truly needs to adapt his or her own understanding of both boats. All people must learn to captain for

themselves, because commercial industries act insanely with their own interests in mind, and legislatures devise only insufficient and temporary fixes. In other words, the only enduring solution is for individuals to construct their own personal rafts with their own viable values regarding privacy in the twenty-first century. As long as the rafts are not made of merely cardboard and duct tape, they will surely be the best hope for enduring this perpetual storm.

Works Cited

Abelson, Hal, Ken Ledeen, and Harry Lewis. *Blown to Bits: Your Life, Liberty, and Happiness After the Digital Explosion*. Upper Saddle River, NJ: Addison-Wesley, 2008. Print.

Batelle, John. *The Search: How Google and Its Rivals Rewrote the Rules of Business and Transformed Our Culture*. Penguin, 2006. Print.

Ku, Raymond Shih Ray. "Privacy is the Problem." *Widener Law Journal* 19.3 (2010): 873-891. *Academic Search Premier*. Web. 16 Nov. 2011.

Magi, Trina J. "Fourteen Reasons Privacy Matters: A Multidisciplinary Review of Scholarly Literature." *Library Quarterly* 81.2 (2011): 187-209. *Academic Search Premier*. Web. 1 Dec. 2011.

Matthew Green, et al. "Security Through Legality." *Communications of the ACM* 49.6 (2006): 41-43. *Academic Search Premier*. Web. 16 Nov. 2011.

O'Harrow, Robert. *No Place to Hide*. New York: Free Press, 2005. Print.

Pariser, Eli. *The Filter Bubble: What the Internet is Hiding from You*. Pengiun, 2011. Print.

"Quotations by Subject." *The Quotations Page*. Michael Moncur and QuotationsPage.com, 2012. Web. 11 March 2012.

Ramsay, Haden. "Privacy, Privacies and Basic Needs." *Heythrop Journal* 51.2 (2010): 288-297. *Academic Search Premier*. EBSCO. Web. 12 Oct. 2011.

Shroff, Marie, and Annabel Fordham. "'Do You Know Who I Am?' Exploring Identity and Privacy." *Information Polity: The International Journal of Government & Democracy in the Information Ae* 15.4 (2010): 299-307. *Academic Search Premier*. Web. 28 Nov. 2011.

Tancer, Bill. *Click: What Millions of People are Doing Online and Why it Matters*. Hyperion,

2008. Print.

Tapscott, Don and Anthony Williams. *Wikinomics: How Mass Collaboration Changes Everything*. Penguin, 2010. Print.

Tavani, Herman T. "Philosophical Theories of Privacy: Implications for an Adequate Online Privacy Policy." *Metaphilosophy* 38.1 (2007): 1-22. *Academic Search Premier*. EBSCO. Web. 12 Oct. 2011.

Weinberger, David. *Everything is Miscellaneous*. Holt, Henry & Company, 2008. Print.