Privacy and the Self:
Privacy in the context of self

Darren Gene Peterson

May 3, 2013

With new additional technological developments, new and difficult privacy issues often arise. Since the pace of technology is so rapid, it is unwise to meet every new technological advancement with new discussions of privacy. Instead, the privacy protections currently in place should cover new technologies. This can be done if we can place new technologies within an existing framework.

In this paper I hope to add some clarity to the discussion of privacy with regard to new technology. I will do this, counter-intuitively, by adding some complexity to our definition of *self*. Taking an expansive view on what is the *self*, to include external augmentations and public personas, is valuable as we weigh the implications of new technologies on privacy. We can use existing norms and laws to guide protections for privacy in regard to new technology by applying the old rules to the new situations. In this paper I propose a framework for viewing privacy with new technological developments that maps the privacy of our current understanding of self to an extended definition of self.

I will dissect the *self* along two axes. First I will look from the body in, and identify the components of the *self*. Then I will reverse course and look from the inside out. Starting with the body and moving out, where does the *self* end and how far can we conceptually extend it? Along each axis I will identify privacy norms and expectations in regards to our physical selves. Then I will identify extensions, often technological, often virtual, that could also be considered part of the self. I will map the existing or expected current privacy norms to the new technical or virtual extensions of the *self*. In addition, within each section I will discuss some limited technological examples. I will keep the technical examples limited because this paper is to be as general as possible with regard to technology. Advances in technology move too rapidly for me to be able to comment on any particular form of technology. Instead, the framework we generate should be

able to accept and provide guidance for any new technology that is examined.

Self

There is a large history of thought on what is the *self*. Where does the *self* reside? How far does the *self* extend? What are the components of the *self*? These are important philosophical questions, the answers to which are not clear. Viewed in the most minimal way, the *self* ends at the extent of the body, but where the body ends is yet another difficult question. Further, there are arguments to be made that the *self* extends beyond the limits of the physical body. For the purposes of this paper, it is sufficient to accept that the location of outer bound of the *self* is contentious. There are many ways to look at the question, each with some validity.[1]

Much of the technology that we create can be considered as part of the *self*. Here, the *self* includes the body and many things around the body, such as the pieces of the body that are frequently discarded (hair or skin), or augmentations of the body (eyeglasses). I define the *self* to include the mind and many things that enlarge the mind, such as the tools used to augment the mind (pen and paper). In addition, the *self* may also include esoteric things outside of the body, such as the faces we apply when we take part in social interactions with other people. In the context of privacy, it is valuable to view the *self* most expansively.

[1] There are many authors to read concerning self. For this paper I recommend Goffman's *The Presentation of Self in Everyday Life*, University of

HISTORICAL CONTEXT

The impetus for this paper was my reading of the Fourth Amendment of the U.S. constitution. Although the word *privacy* is not mentioned in the Fourth Amendment, it is typically regarded as the basis of privacy in the U.S. The amendment is very short. It consists, basically, of a list of several things that are protected from search and seizure.[2]

The items listed in the Fourth Amendment can be considered, at least partially, as components of an expanded *self*. Comparing these components with contemporary examples provides guidance for when and where contemporary technologies are to be considered part of the self, which in turn provides guidance on what privacy protections should be created for each new technology. This can gives some historical context to our discussion of privacy.

Persons. The first item on the list is persons. I read this to mean that either the body is protected or the *self* is protected. Both are true and obvious.

The contemporary technological advancements of the body are augmentations and prosthetics. Tools implanted within our bodies, such as pacemakers, should receive the same protections as our bodies. It is less clear what protections external prosthetics should receive.

Papers are extensions of our minds. We use tools (technology) to expand our minds. One of the most simple of these is paper and pen. When we write, we write to expand our minds. We can capture ideas that we would otherwise forget, explore multiple ideas simultaneously, compare and contrast ideas, ruminate on them, and return to them. As a journal, our papers are used to facilitate thinking, and so are as part of us as anything. In some ways, our written thoughts may even be more us than our bodies, since they are extensions of the mind.

---

[2] The complete text is: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized"
http://en.wikipedia.org/wiki/Fourth_Amendment_to_the_United_States_Constitution

Some current versions of *papers* are online data storage, and the hard drives or other digital storage devices that we use. Currently the physical versions of these (e.g. pen drives) get the same privacy protections as papers, but the online versions (e.g. cloud storage) do not. I will discuss privacy and self with regard to body and mind at greater length later in this paper.

House. I would argue that there is a connection to *self* in the barriers that we erect around us. Part of being human and a self is to have expression written upon our bodies. These expressions are deserving of privacy protections. In this regard the house is like the makeshift home of a hermit crab. It is a layer of skin to protect the body from the environment. If a roof over your head is to protect your body and life, the walls serve the lesser but still important job of shielding you from the view of society.

Homes have not changed much since the time of the Founding Fathers. Houses are by definition very physical. A contemporary corollary can be seen in the location and protection of our digital selves. What are the houses of the online versions of our *selves*?

Effects are a subset of property. They are the collection of small things that we possess, such as clothing or furnishings. Depending on your materialistic views, effects are not part of the self. But there are exceptions in things like totems, and nostalgic items. Humans tie memories to objects. In a way, our personal effects are physical repositories of our emotions.

As we spend more of our time online, more of our memories are tied to virtual effects. Treasured photos stored online should have all of the same privacy protections as photos stored in shoebox in my closet.

Considering whether each protection granted in the Fourth Amendment could be viewed as a part of the *self* helps to clarify where the new technologies and what privacy protections they should receive.

PART 1: FROM THE BODY IN

Body

I have created a taxonomy of contexts of privacy concerning the body, which can be found in the Appendix.

Mind

It is a safe assumption that the mind can be considered part of the *self*. Perhaps the mind is where the *self* resides. To say more than that we get back into the difficulties that we faced with the definition of *self* earlier. I will not go into detail here about just what and where the mind is. I will focus instead on the relationship of privacy to the mind.

The Fifth Amendment protects us from self-incrimination. In a way this is a protection of privacy of the mind. We cannot be compelled to use the information in our heads against ourselves. In two recent court cases, Fourth and Fifth Amendment protections concerning whether a defendant can be compelled to divulge the password for an encrypted hard drive were tested. In one, a California man was protected from being compelled to divulge his password. In another, a Colorado woman was forced to divulge her password. In both cases the laptop that contained the hard drive was seized with a valid court order.

In the latter ruling, the prosecution argued that "if the defendant is not compelled to unlock her computer, that would amount to a concession to her and potential criminals ... that encrypting all inculpatory digital evidence will serve to defeat the efforts of law enforcement officers to obtain such evidence through judicially authorized search warrants, and thus make

their prosecution impossible"[3]. While in the former ruling, the 11th U.S. Circuit Court of Appeals laid out the following reasoning:

> First, the decryption and production of the hard drives would require the use of the contents of Doe's mind and could not be fairly characterized to a physical act that would be non-testimonial in nature. We conclude that the decryption and production would be tantamount to testimony by Doe of his knowledge of the existence and location of potentially incriminating files; of his possession, control and access to the encrypted portions of the drives; and of his capability to decrypt the files.
>
> Requiring [the defendant] to use a decryption password is most certainly more akin to requiring the production of a combination because both demand the use of the contents of the mind, and the production is accompanied by the implied factual statements noted above that could prove to be incriminatory.[4]

The reference to a combination lock is relevant. It comes from a 1988 Supreme court ruling in which Justice Stevens mused that a key to a lock can be compelled from a defendant, but a combination to a lock cannot.[5] It is part of the mind argues Justice Stevens:

> A defendant can be compelled to produce material evidence that is incriminating. Fingerprints, blood samples, voice exemplars, handwriting specimens, or other items of physical evidence may be extracted from a defendant against his will. But can he be compelled to use his mind to assist the prosecution in convicting him of a crime? I think not. He may in some cases be forced to surrender a key to a strongbox containing incriminating documents, but I do not believe he can be compelled to reveal the combination to his wall safe – by word or deed.[6]

A defendant cannot be compelled to use his mind to incriminate himself.

In a way it is privacy of the mind that the Fifth Amendment protects. But in these two cases the protection from self-incrimination is not about protection from search of the mind exactly, but about using the mind to self-incriminate. This is a more nuanced view than privacy

---

[3] http://www.wired.com/threatlevel/2012/01/laptop-password-5th-amendment/

[4] http://www.wired.com/threatlevel/2012/02/laptop-decryption-unconstitutional/

[5] http://blogs.denverpost.com/crime/2012/01/05/why-criminals-should-always-use-combination-safes/3343/

[6] John DOE, Petitioner v. UNITED STATES. 487 U.S. 201 No. 86-1753. June 22, 1988

of the mind directly. Compelling a defendant to do some action that is not testimonial is allowed, but compelling incriminating testimony is not. As these two cases show, it is currently not clear when passwords are protected by the Fifth Amendment.

One hopes that this matter is resolved quickly in light of another emerging technology:

> A new study… found that sensitive personal information, such as PIN numbers and credit card data, can be gleaned from the brainwave data of users wearing popular consumer-grade EEG headsets. A team of security researchers from Oxford, UC Berkeley, and the University of Geneva say that they were able to deduce digits of PIN numbers, birth months, areas of residence and other personal information by presenting 30 headset-wearing subjects with images of ATM machines, debit cards, maps, people, and random numbers in a series of experiments. [7]

Here we have the introduction of a powerful new technology. Assuming that this technology is still in its infancy, we can expect the privacy complication due to this technology to only grow.

This leads to the question: when should the government be allowed to search and seize information in your mind? The two cases referenced above are more about Fifth Amendment self-incrimination issues than privacy, but the compelling of the divulgence of passwords come dangerously close to demanding a search of the mind. With the addition of the technology to read minds, we suddenly find ourselves with new search method without much privacy protection in the form of precedent.

Here is an example of insufficient privacy protections for our current, traditional understanding of self. It is clear that we are not to be forced to testify against ourselves, and that our bodies are protected from search, in most cases. The mind is more core to the self than the body and so deserves all of the protections of privacy granted to the body and more. We must clarify just what protections the mind is deserving of now. Then we must attempt to extend those

[7] http://www.wired.com/threatlevel/2012/08/brainwave-hacking/

privacy protections to our technologically extended selves.

A contemporary technological corollary to the mind is online data storage. Cloud computing, or other online data storage methods, is a way to store your data, of any digital type, on remote servers accessed over the internet. Like the papers referenced in the Fourth Amendment, cloud computing is an extension of our minds. We use, or can use, this online data storage as a way to expand our ability to remember and to think. Cloud storage is an augmentation of our minds and therefore should be afforded the same privacy protections.

If the case law eventually gets resolved, and we have clear rules on if or when the contents of our minds can be accessed, then we can apply the same rules to the contents of our data stored in the cloud. Or if not the same, the rules that we generate should have reverence to the earlier bodily derived case law.

PART 2: FROM THE BODY OUT

We've delved into our most core of cores exploring body and mind. Now we will reverse course. We will start at the body and move outwards. Here, we will explore just where the *self* ends and where the environment begins. Up until now our definition of body extends from our internals to our surface. The extent of my physical body is the tips of my fingers or the ends of my hair. But the self does not end there, at least not completely. The *self* also includes, in some cases, our interactions with the world, the personas we create, our information about *self* outside of the *self*, and more. There are multiple ways to look at the extremity of the body.

Here I will explore some possible *selves* outside of the body. First we will explore *face*, or impression management, and the ways in which managing how you are viewed is both *self*

and deserving of privacy consideration. Following that we will explore waste, both physical and digital, and our social interactions. We will consider when each can be considered part of the self and how much each is deserving of privacy. Finally, we will explore how our social interactions could be considered part of our *selves*.

Face

In every social interaction there are faces, or presentations of self, that we each create and present. "Through our *presentations of self* we engage in *impression management*, sometimes using space (e.g. *frontstages* and *backstages*) to organize what we do and do not let others know about us."[8] We devote an amazing amount of interaction to maintaining and managing ours and others' faces.

Privacy is an important part of face management. We do not allow everyone to see everything about us. In fact, it is through the careful management of how much of ourselves we reveal, or what part of ourselves we reveal, that is the bulk of face management.

> At its core managing privacy is about managing relationships between ourselves and others. Altman for instance refers to privacy as a 'boundary regulatory process by which a person makes himself more or less accessible to and open to others.' (Nippert-Eng, p.22).

---

8 Christena Nippert-Eng. *Islands of Privacy*, University Of Chicago Press, 2010. p. 24

The convention I will use for noting referenced material will be the standard footnote, as we have seen so far. Except that I will use a separate convention for the materials that were assigned for the class. The class being, of course:

SOC 425-001 **Privacy**, Spring 2013
by Dr. Christena Nippert-Eng , Professor of Sociology
at the Illinois Institute of Technology, Chicago, IL

For the assigned texts, I will use an endnote with only the author's last name and the page number of the reference. In addition to Nippert-Eng's book, listed above, the books assigned in class were:

Robert Ellis Smith. *Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet*, Privacy Journal, 2004.
Ellen Alderman and Caroline Kennedy. *The Right to Privacy*, Vintage, 1997.
Daniel Solove. *Nothing to Hide: the false trade-off between security and privacy*, Yale University Press, 2013.
Helen Nissenbaum. *Privacy in Context: Technology, Policy, and the Integrity of Social Lif*e, Stanford Law Books, 2009.
Lori Andrews. *I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy,* Free Press, 2013.

We present a version of ourselves, a proxy for each social interaction. We try on different roles in the group dynamic, some more successful than others. We keep a stock of social selves and select one depending on the situation. "In the course of people's lives we act and transact not simply as individuals in an undifferentiated social world, but as individuals acting and transacting in certain capacities as we move through…distinct social contexts." (Nissenbaum, p. 129). It is through this layer of masks, filtering out the hidden private self underneath, that we manage our social interactions.

Regulating accessibility equates to regulating access. We maintain filters though which we allow only fragments of our selves to show though. The privacy of these filters is required for a healthy society. "We cannot know completely the individuality of another… It is impossible … to see anything but juxtaposed fragments." (Simmel, in Levine, in Nippert-Eng, p.22). Without the ability to put up faces, to hold back information, we would lose control of our relationships.

> We eventually learn that what others do and do not know has consequences for us and our desired relationships with them. Others will allocate to and withhold from us all kinds of support, opportunities, and resources based on whatever fragmentary knowledge they have of us. It is precisely this desire to shape our relationships with others in particular ways that makes controlling what they know of us so important to us. (Nippert-Eng, p.23)

It is this management of face through privacy that allows us control over who we are at any moment, or in any given context. It is through privacy that we exercise autonomy of the self.

According to van den Hoven, moral autonomy is the "capacity to shape our own moral biographies, to reflect on our moral careers, to evaluate and identify with our own moral choices, without the critical gaze and interference of others and pressure to conform to the 'normal' or socially desired identities." (Van den Hoven in Nissenbaum, p.81). Autonomy is the option to exercise self-control, the choice to be the way you want to be. It is the possibility to create your

own self in the way that you prefer. Autonomy is the granting of free will.

Nissenbaum, in "Privacy in Context," describes three different ways in which privacy and autonomy are interrelated. First, privacy is a form of autonomy. In this connection, privacy is a method through which we define ourselves. Second, privacy frees us from self-censorship. When we know that we are bing watched we act differently, thus being watched reduces our autonomy. Third, privacy protects us from the "panoptic sort." This is Gandy's term for the combination of inequality and aggregation of information - that can limit the options of the less powerful. (p.79)

Privacy is the method through which we define ourselves. Nissenbaum referencing Goffman and Austin, says that, "Privacy constitutes the capacity to shape how individuals define themselves and present themselves to others in the variety of life's circumstances and as such, the capacity to express an important dimension of autonomy, or self determination." (Nissenbaum, p. 82). Since we control the information that others see or know about us by hiding certain pieces at certain times, it is through privacy that we shape the impression that others have of us. We need to have the control of the flow of information about us in order to control the impressions of us that are held by others.

Privacy frees us from self-censorship. When I am watched, I no longer act in the same way as if I was alone. The very act of being observed has an effect on the actions of the person being observed. knowing that others are watching and recording forces us to self-censor. We limit our actions to those that we believe are safe or acceptable. Worse, this self-censorship can continue even if we are not actually being watched.

> "As long as we are being observed, monitored, and possibly judged, constantly taking others into consideration in determining courses of action and decisions, our actions are not truly voluntary. But there are also indirect disciplining effects that we know to be embodied in the fundamental notion of a panopticon, for even

> when we are uncertain whether or not we are being watched, we must act as if we are. When this happens, when we have internalized the gaze of the watchers and see ourselves through their eyes, we are acting according to their principles and not ones that are truly our own. (Nissenbaum, p. 82)

It is possible that it is even worse that this. Not only our actions, but our thoughts can change when we live with the assumption that we are being watched. For example, the movie *The Lives of Others* takes place in Soviet-era East Germany. In the movie, the protagonist is being watched by the stasi, or secret police. They tapped his phone line and installed "bugs" in his home. Suspecting that he was being monitored, he tested his suspicion by aiding in the escape of a friend. Although he was vocal about his help both at home and on the telephone, he was not caught. After running the test and "knowing" that he was free from observation, the protagonist's demeanor changed. He was free to let his mind wander into areas where before he had feared to go. Not being afraid to say things that could get him into trouble allowed him to think creatively and deeply. He was not constantly interrupted by self-censorship. He was not limited in his thoughts to only those that are accepted.

The third way in which Nissenbaum connects privacy to autonomy is in the panoptic sort. The panoptic sort is a term coined by Gandy to describe the process of how unequal access to information and the sorting of people into categories leads to unequal opportunities. This limit on our autonomy is more subtle. It works as follows. Vast amounts of information is collected about us through monitoring and recording. This can happen in many ways, through medical records, tax records, payment histories, and so on. This information is collected and shared; it is put into a large database that analyzes the information of many people in aggregate. Then that data is used to categorize us. Depending on your past histories you could be categorized in many different ways. This will be discussed further in the next section, starting with the physical version of the panoptic sort, and continuing into some digital examples.

WASTE

At what point do components of our bodies stop being part of our bodies? When do they stop being part of the self? In every microscopic piece of dead skin that forms the dust in the air is the compete genetic information of the person who once owned it. The genetic information can be used to identify the individual from where it came. Or, in some cases, can even re-create that person, or a clone of that person. Anything that is tagged with our genetic information, anything that can identify us or re-cerate us can be considered in some way as part of the *self*.

The movie Gattaca takes place in a future world where genetic science has advanced to such a degree that decoding and manipulation of our genes is commonplace. In this world, parents screen their potential offspring to ensure that only the best and strongest specimens are born. A scoring system for genetic prowess forms. Since reading of genetic codes is quick and easy, people are regularly scanned to verify their identity. This leads, in the movie, to a stratification of class based on genes. This class system is informally enforced through genetic monitoring. We watch as the protagonist, a member of this sub-class, excels through subterfuge. Through careful hygiene he hides his genetic tracks. These include all bodily cast-offs, such as hair, eyelashes, or fingernail clippings, that the body regularly discards. He purges himself of these identity markers every morning and replaces them with false ones. Eventually the rigors of constant self monitoring overwhelm him and he is discovered.

Gattaca takes place in an imaginary high-tech future, but the technology for most of the monitoring currently exists and is in use. The combination of this constant ridding of genetic information, along with the technological ability to collect, read, and store the information, supports a system where a person's opportunities may be limited by their genetic profiles. Employment opportunities, health insurance, or even access to the same entertainment options as

everyone else may all be withheld to one class of people based on their expected fitness.

Lori Andrews details how this technology has already raised serious concerns. Doctors testing for one thing can scan for many, and do, thinking that there is no harm. But when employers or insurance companies get the scan data, and predictions of future medical ailments, they have discriminated against the patients. “With certain genetic mutations, for example, some women had a higher risk of developing breast cancer than other women. Even with those mutations, half the women would not develop breast cancer.... [E]mployers and insurers wanted that information to make their decisions. There were no legal limits on what could be done with that information.” (Andrews, p. 53).

Because this is about physical things – your body and the genes it contains – the privacy debate around this issue is more clear cut. We understand, for the most part, how it works: a piece of our bodies can be analyzed to make predictions about our health. Many people find this technology disconcerting and have reactions to it. But eventually laws change to catch up with the technology. “Since then, Congress has passed a law specifically prohibiting employers and insurance companies from discriminating against people based on the results of genetic tests.” (Andrews, p. 54) There are an analogous events happening currently for our digital selves. Here knowledge about the invasion of privacy is not well known, and since this is digital and not physical, what to do about it is unclear.

The corollary to physical waste for our digital selves is called “data exhaust”. Data exhaust is the byproduct of our interactions with modern sensors that collect and store data about the interaction. The most common is simply surfing the internet. As we connect to websites, data is stored on our computers and other places in the internet. This data tracks every page that we visit and much else about our habits.

Unlike for our physical selves, the entirety of this information is hoovered up and stored. "One such company has and average of 1500 pieces of information on each person, everything from their credit scores to whether they've bought medication for incontinence." (Eli Pariser, in Andrews, p. 35) The difference between physical waste and data exhaust is that data exhaust has value. (Andrews, p. 39) Companies collect data from many users and compile it. After analysis, patterns can be found in the collected aggregate data. These patterns inform companies on how to respond to their customer base.

Valuable or not, is it appropriate to collect the waste of our digital selves? Returning to Gattaca, the bodily data that was gathered was used in many suspect ways. Gather a hair from a potential lover to determine their fitness as a mate. Use the mandatory company drug test to screen potential employees for physical or mental aptitude, or future health complications. We reject these uses of our bodily data out of hand.

Yet the exact same things happens to our digital selves today. "The massive acquisition of information by data aggregators, their analyses of it, and their sale of it not only invades your privacy but also denies your individuality and can harm you emotionally and financially. Your private data is not being used just to sell you products but to deny you certain opportunities." (Andrews, p. 35)

Companies that collect and package your information are casting you into one of their pre-formed molds. You have no choice, as things currently stand, to shape your own image, but are forced to be one of the options that they assign to you.

> "Data aggregation and behavioral advertising run contrary to some fundamental social values. Under the US Constitution and civil right laws, institutions are supposed to make decisions about people based on their individual characteristics, not because of aggregated data that assumes that people who are in a certain demographic are more likely to do X or Y…. A person must be judged on his or her own merits." (Andrews, p. 36)

Inequalities of power combined with unequal access to information leads inevitably to discrimination. And in the case of online data, our personas are not only made for us, but made based on information that we don't even know was collected, made in secret so we don't even know what personas exist or how many of them there are, and if we did we would not have the ability to change them anyway.

In the realm of waste, privacy law needs to be improved, for both physical and data privacy, to match current social norms. We are distressed by the idea of our bodily data being collected without our permission and used in ways that deny us opportunity. We want protections from this sort of invasion. We should also demand protections for our digital selves, so that we are not denied opportunities based on our digital profiles.

The difference between face and waste is in denying your right to make your own self versus denying you opportunities based on your profile. Face is about individuality and autonomy over your own identities - whether we make our own personas, or if they are made for us. This is denying you control over your representation of your individual self. Waste is about aggregating data and sorting people into profiles and discriminating. When our waste is collected and sorted, aggregated and analyzed, the analyzers create their own digital buckets and then stick your digital self into one or more of them.

Social Representation

In 1890, two Boston lawyers wrote an article in the Harvard Law Review expressing outrage over new technologies, their use by unscrupulous newspapers, and the increasing invasion of privacy. They were Samuel Warren and Louis Brandeis, and their article had

immense implications on the discussion of privacy in the US. The impetus for their persuasive article was the rise of two new technologies.

First was the invention of "dry plate" photography. This new photographic technology allowed truly instantaneous photographs. Suddenly amateur photographers everywhere could take "snapshots." According to Bill Jay,

> To this date the history of photography had never experienced such a shock wave of change. No longer was photography the prerogative of the trained professional or reasonably well-educated and wealthy amateur. Now photography was "child's play" which "a person of average intelligence could master in three lessons." Thousands upon thousands of amateurs now became their own photographers – and wreaked havoc in the medium. By 1900 it was estimated that there were four million "camera fiends" who were "kodaking" everywhere and creating a major social nuisance of themselves in the process of filling their albums.[9]

Paired with the invention of instant photography was the advent of national newspapers. Gossip that was once only whispered around the town, or perhaps printed in a local paper, was now being pushed out to a large audiences. "Prior to the Civil War, news reporting was … 'small beer and scandal'; now it was a wholesale enterprise, whether or not the subject matter was especially newsworthy." (Smith, p. 126). Included now with the gossip were the surreptitious snapshots of new photographic technology.

> Imagine the shock, for the first time, of having a stranger take a photograph of you without any warning and without you knowledge or permission. …Then imagine the possibilities of instantaneous reproduction of those images in newspapers circulated throughout the country - never before remotely possible. All of this future shock occurred within a span of fewer than 45 years. (Smith, p. 126)

With the combination of these two technologies came a surprising invasion of privacy. People suddenly found that, when in public, they could have their image recorded and printed

[9] http://www.billjayonphotography.com/The%20Camera%20Fiend.pdf

later in newspaper dailies. This came as a shock to the gentried class – the people most likely to be photographed – who up to this point had the most privacy and lost the most privacy with the change. And of course had they had the power to do something about it.

Which brings us to Brandeis and Warren's article. They felt that there should be some legal remedy for the invasion of privacy they felt when they found themselves gossiped about in newspapers. They wrote:

> Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops." For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons.[10]

With this article, a new area of privacy protection began to form. Brandeis and Warren laid out the "right to be let alone."

This article had great influence over the years in the privacy debate. It significantly expanded what we think of as privacy, and began the legal defense of these new forms of privacy. Of particular interest here is the right to representational privacy.

Brandeis and Warren's article and their desire to be let alone can be seen as a demand to control their representations in public. What they are demanding is the right to variants of *self*. When they say that they want to be left alone, they are saying that they want the right to not have to be their public selves.

According to Warhol, we each get 15 minutes of fame.[11] Although it seems like we all want it, in fact it can be exhausting to be in the limelight. Even those who are in it do not want to stay in it continuously. Eventually one must step out of the limelight, get away from the public's

[10] Warren and Brandeis, The Right to Privacy, Harvard Law Review. Volume IV, December 15, 1890.

[11] http://en.wikipedia.org/wiki/15_minutes_of_fame

attention and be in their private space. Have private time. Brandeis and Warren, when they demand to be let alone are demanding the chance to be themselves. Or rather, to be some other self than their public self.

There is a current corollary to the invasion of privacy that Brandeis and Warren felt then, in the realm of our online digital representational selves today. Our privacy is again invaded by "kodakers." But instead of Kodak, it is Facebook and other social networks that are enabling this invasion of privacy.

Today we are all public figures. Anyone who maintains a Facebook or Twitter account is creating a public version of themselves. There are many reasons to create a profile on a social network. Facebook is a communication tool. Flickr is a way to store creative content. But an important purpose of every social network is in creating a social profile. We create a self – an online digital self – when we create a profile.

Andrews offers compelling example in a story about a former small town high school student and an ode to her hometown that she posted on MySpace. “The ode, which she took down six days later began, ‘The older I get, the more I realize how much I despise Coalinga.'" The ode, later printed in the small town’s newspaper, lead to many unfortunate circumstances, including death threats, shots fired at the family’s home, and the loss of her parents’ trucking business. (Andrews, p. 55) At issue here is the small town’s newspaper printing the MySpace posting. The courts, when they eventually ruled on the case, determined that no one has a reasonable expectation of privacy for a posting on a public social website. In many ways this makes sense – it is a public social website after all. If the ode is considered creative content, if it is her property, then newspaper might be at risk of violating copyright law by publishing the ode, but the paper shouldn’t have to worry that it is a privacy violation. If we look at it from another

context, that she was articulating her online social self, then there is a compelling case for it to be considered a violation of privacy.

Beginning with Brandeis and Warren's article, the use of your physical representation without consent slowly became included into the definition of invasion of privacy. In the case of the "Ode to Coalinga," the student's representational privacy was also violated. Her postings on MySpace were not for gain, or to further discussion, or food of thought. She was not trying to influence anyone or make a point. She was simply expressing herself. This expression of self was done in order to create a version of her digital representation.

The things that we post on social sites are intended as a way to create our representational digital selves. They are more similar to exposing or creating a piece of our personalities than to driving at making a point or creating new knowledge. Facebook and other social networking sites a places where people can represent themselves. We post our images, but that is only part of what defines the shape of that self. We post our likes and dislikes, our friends, our families, and our interests. People spend significant amounts of time crafting profiles that express the person that Facebook user's what the world to see them to be. With this in mind, I posit that the Ode to Coalinga was written less as a critique of a small backwards town and more an expression of a student attempting to show that she is more and better than where she came from.

Communication

"Gergen (1991) believes that the very concept of self is becoming defined more thoroughly by relationships…

> In this era the self is redefined as no longer an essence in itself, but relational. In the postmodern world, selves may become the manifestation of relationships, thus placing relationships in the central position occupied by the individual self for the last several hundred years of Western history. (Gergen, in Nippert-Eng, p. 209)

"The infidelities of the post office and the circumstances of the times are against my writing fully and freely. I know not which mortifies me most, that I should fear to write what I think, or my country bear such a state of things," Thomas Jefferson wrote in 1798. (Smith, p. 50). Since at least 1782 in America (1710 in Britain) letters were protected as confidential. Clerks could not "open, delay, detain, secrete, embezzle, or destroy" any letter without a warrant. (Smith, p. 50) This was later applied to all persons; in 1825 the federal law protecting privacy for and from all people was enacted. People didn't feel the confidence in the privacy of the post until later, when the adhesive envelope was created. (Smith, p. 56)

US Supreme Court justice Joseph Story called intruding into the privacy of personal correspondence 'odious'. "It strikes at the root of all that free and mutual interchange of advice, opinions, and sentiments, between relatives and friends, and correspondents, which is so essential to the well-being of society, and to the spirit of a liberal courtesy and refinement." He went on to say that it would, "compel everyone in self defense to write, even to his dearest friends, with the cold and formal severity with which he would write to his wariest opponents or his most implacable enemies." (Smith, p.51)

At the heart of the matter is candor and self-censorship. If we believe that our communications are not private, or cannot be made private, then we will censor those communications. The interaction, the discussion between two correspondents would be diminished. Without an open dialogue there cannot be true expression. Without privacy one's social representation is incomplete.

The letter is a physical representation of our representational self. In a way, we can look at it in analogy to a person and his house. When the letter is considered to be another self, a manifestation of the our attempt at communication with another, then the first class envelope in

which it resides is the letter's house. And similarly to a person's home, a letter's envelope does not have the expectation of privacy. But the contents within are private. Including the inside of the envelope and any effects contained within the package.

This may seem obvious in the case of a written letter, but becomes less clear and more complicated in the case of electronic communication.

There are however still some protections for the outside of the letter. These are similar to the protections of our physical self. There are limitations on how our representations can be used. Envelope information can't be collected and disclosed. Information gathered for one purpose should not be used for any incompatible purpose. (Smith, p.56)

We have, internally, layers of the body and mind, and many ways to augment them. All of these, body, mind, and augmentations of body and mind can be considered the self. In addition, there are aspects of the self that are external to the body. Our presentations of self (faces), discarded parts of the body (waste), and our social representations are all part of the self. Many new technologies are actually augmentations of these selves. Our Facebook profiles and the assigned profiles generated about us from our data exhaust are examples of our external, extended selves. If we consider our traditional, existing augmentations as part of our selves, and consider the privacy protections granted to them as privacy protections granted to our selves, then when we create new, technological augmentations we can use our existing protections to guide what new privacy protections to grant.