ASA

Annie Searle & Associates LLC

## Research Note

# The Conflict of Privacy and Disclosure Law

## The Criticality of Minimizing Collateral Data

By Matthew Christian



Keywords: privacy, data collection, government

*Abstract: This research note discusses the complex issues surrounding data collection and subsequent privacy issues. In particular, the paper explores the issues surrounding data collection by government agencies and public disclosure laws.*

### Privacy

> *"A person's "right to privacy," "right of privacy," "privacy," or "personal privacy," as these terms are used in this chapter, is invaded or violated only if disclosure of information about the person: (1) Would be highly offensive to a reasonable person, and (2) is not of legitimate concern to the public."*
>
> *RCW 42.56.050*

Privacy is a complex topic. Privacy is one of those words where it is difficult to define without using it in its own definition. What is considered private changes with time and circumstance, and even more from person to person and from culture to culture. Privacy is often considered an inalienable right along with life, liberty, and the pursuit of happiness, though it is not explicitly defined in the Constitution. It can be traded away willingly or taken away as a consequence without issue, but if it is taken without being asked is treated in the same regard as basic human rights.

Privacy in the Information Age is a seemingly fleeting thing. Technology has enabled advanced communications and services that have made us better connected and informed, but as the saying goes, there is no free lunch. The same systems that connect us and inform us track our behavior and goings-on. Fortunately, market pressure has encouraged private companies to disclose what information consumers are changing and to offer and opt-out option if so desired, leaving consumers with a degree of control

enabled by informed consent. This same degree of control does not hold true when examining image data held by government entities, especially with recent advances facial recognition software.

The single unifying element in all definitions of privacy is *informed consent*. In the context of information, informed consent is involved with making a person aware of what information is going to be collected and how it will be used.[1] Without informed consent, an individual has no opportunity to protect his privacy, even if the data being collected is seemingly innocuous. It is in informed consent that the Washington State law fails and exposes its citizens to privacy violations granted through image and video captured for other purposes. The majority of the following discussion is focused on how public disclosure laws allow citizens to gain access to much more information about each other than historically available due to public disclosure law.

**Public Disclosure Law**

In the U.S., the Freedom of Information Act[i] grants citizens access to federal records, and each state also maintains local public disclosure laws, which can vary from state to state. Liberal public disclosure policies are an essential cornerstone to a healthy democracy. Public disclosure laws not only inherently improve the behavior of public agents simply by the knowledge that most records are accessible to the average citizen, but also provide the means for a democratic society to govern itself in the manner that it chooses to be governed. The introduction of video recording technology and the rapid improvements in video hardware and software has opened a new frontier for monitoring public agents. However, as with any new powerful technology, the benefits may not always offset the cost.[ii]

> *"The people of this state do not yield their sovereignty to the agencies that serve them. The people, in delegating authority, do not give their public servants the right to decide what is good for the people to know and what is not good for them to know. The people insist on remaining informed so that they may maintain control over the instruments that they have created[iii]…" RCW 42.56.030, Washington State*

The principle of public record disclosure law in Washington State is stated in very clear terms; that the

[i] More information on the Freedom of Information Act can be found at http://www.foia.gov/

[ii] All references to "law" in the rest of this paper will be in reference to Washington State Law unless otherwise noted

[iii] Remaining text of RCW 42.56.030 goes on to explain how the policy was written.

government put in place by the people is subject to monitoring by the people. This is supported by RCW 42.56.010, which defines public records in such a way that essentially all content generated by a public agent is subject to public disclosure law. RCW 42.56.040 further supports this principle by requiring all public state agencies to make the process of requesting public records easily accessible and understandable.

The state does grant a few exceptions to a select population of records. RCWs 42.56.230 and 42.56.240 outline specific parties and situations that are exempt from the public disclosure laws. These groups include minors in public schools, patients in public health agencies, victims of crime, undercover police officers, and other groups. These statutes also restrict the disclosure of state-issued identification records that could be used in combination with other records to determine the identity of a protected group.

Now that the foundations of public disclosure laws have been explained at a high level, we can start to examine how image data complicates the issue. The scope of public data is very wide. It encompasses every record generated in every public office across the state. Some examples at the state level include the Liquor Control Board, Department of Natural Resources, and the State Board of Education. Each department, at both the city and state level, requires certain types of data in order to carry out its intended function. These departments are given the authority and resources to collect said data, and by default, are required to disclose that data to the public with the exception of exempt records.

Collecting data to support public agencies empowers public agents to make fact-based decisions that better the lives of the general public. Critical utilities, such as transportation and power, and public services, such as libraries and education services, function largely in part to the data that each agency is able to collect. Data collection is also essential to the public maintaining a watchful eye on the conduct of government agents. The concern at hand is not with agencies gathering essential data, but on the imprecise nature of image data[iv] that is being used at larger and larger scales and how it compromises the identity of protected citizens as well as the privacy and well-being of the general public.

## Collateral Data

Technology can only be as smart as it is programmed to be. No matter how sophisticated the machine learning algorithm or coding, technology is still reliant on a person for guidance. Image capturing devices

[iv] Image data includes video and photograph media

are no different. A camera captures all data in its lens regardless of the intent of the photographer. To the information scientist this additional contextual information is classified as *metadata*, or as Darin Stewart describes it in his book *Building Enterprise Taxonomies*, reference information not indicated explicitly in the content itself, but rather is supplementary to it. In other words, metadata is information "about" the data element that is not necessarily a part of the data element itself.[2] Metadata is what powers search algorithms, indexing functions, and data mining; it is the thing that makes information work.

Images are intrinsically rich with metadata. The phrase "a picture is worth a thousand words" is an excellent representation of the amount metadata that can be derived from a single image. Herein lies the problem. The imprecise nature of a camera and metadata-rich characteristic of an image generates large amounts of *collateral data*[v], data elements that, through intentional or unintentional means, are collected in addition to the specific data element being pursued that are not relevant to the purpose of the data collection process. The types of images being recorded vary widely by public office or department, yet the issue persists throughout. Each image will often include data that is outside of the scope of the purpose of collecting the data in the first place.

Metadata is only useful to a computer if it is coded in such a way that a software program can read it. This has, historically, been the primary challenge for managing metadata sourced from images because each image needed to have metadata entered manually. Modern technology is quickly negating that roadblock, most vividly exhibited in facial recognition software. The social media giant Facebook is able to automatically "tag" a person in a picture with 97.25 percent accuracy, only 0.28 percent lower precision than humans.[3] The capability to mass-analyze images has significant implications to protecting personal privacy for both the public and for specially protected groups.

As an example, look at Seattle parking police' practice of capturing images of cars parked in public places on a daily basis. This data is used primarily to track automobile movements throughout the city and to track parking utilization. A typical Seattle resident might agree that having the parking police take picture of the public parking spots where she parks on a daily basis is not offensive and that it would probably be of general interest to the public transportation system. However, if that same person were to find out that her abusive ex-boyfriend was able to use those same images to find where she worked and her daily

[v] I mentioned collateral data in an earlier short paper, but never defined it

schedule, her opinion might change.

Police brutality has been the subject of many headline releases in recent years,[4] spearheading additional efforts to monitor behavior in police departments across the state using body-mounted cameras. An incident on August 30, 2010 in Seattle highlights where a body-mounted camera may have been useful in determining what actually happened in a tragic event. John T. Williams, a Native American woodcarver, was shot and killed by a police officer in Seattle, Washington. Williams was walking down a sidewalk in downtown Seattle working on a wood carving with a small knife when he was approached by officer Ian Birk. Williams reportedly refused to put his knife away after being instructed to do so by Officer Birk. After a short but tragic series of events, John Williams was shot to death, and Officer Birk resigned immediately.[vi5] The only video record of the event was the dashboard camera in Officer Birk's police vehicle. The video was able to capture some audio, mostly from Officer Birk, and was only able to show Williams walking across the street with the knife in his hand and Officer Birk exiting the vehicle and following Williams down the sidewalk[vii].

This tragic incident, and others such as the August 9th, 2014 shooting of Michael Brown in Ferguson, Missouri has ignited support for increased deployment of body-mounted cameras in police forces across the country. Private companies like Taser[viii] seem to be ready to fill the need with a well-designed product, and there only seems to be support in the local communities for monitoring police activity. In fact, a pilot program in Rialto, CA saw a 60 percent reduction in use-of-force and 88 percent reduction in complaints against officers.[6] At the surface, this program seems to work extremely well and conceptually makes sense. A police officer is a highly visible, highly impactful government agent who is constantly placed in tenuous situations, so what harm could there be in monitoring police officer activities with video cameras?

The answer has two conflicting sides. The community benefits from monitoring police officer behavior through video. Both citizens and officers behavior is modified in knowing that each is on video and cases are resolved much more rapidly. This practice is fully supported by Washington State law and by the

[vi] More details on the John T. Williams shooting can be found at http://seattletimes.com/html/localnews/2012784234_copshooting02m.html

[vii] The dashboard camera video was posted on YouTube.

[viii] More information on Taser products can be found at http://www.taser.com/products/on-officer-video/axon-body-on-officer-video

principles that citizens should monitor their government. What is *not* beneficial, however, is posting uncensored video of the citizens' interactions with police officers. As an example, the police department in Bellingham, Washington has also started to pilot body-mounted cameras for its police force. An unidentified citizen has started requesting every second of footage from the officer-mounted cameras in Bellingham and is posting those videos to YouTube. One such video contains footage of a bust of a prostitution ring, including a half hour interview with what appears to be a victim of the prostitution ring. This person's name and details of her life story, details that she may not have wanted to share with the public, are now on YouTube for everyone to see.

Another minor problem with body-mounted video is that recording a conversation requires the consent of both parties[ix]. Officers can accommodate the legal requirement by stating that the interaction is being recorded, but that may not always be feasible. Consider an on-foot pursuit of a convenience store robber. Should the officer notify the suspect that their conversation would be recorded while in pursuit through alleys and backyards?

### Legal Conflict

This exact scenario will be played out for every single interaction between citizens and police officers, which raises conflicts in at least two statues. The first direct conflict is with RCW 42.56.240, which exempts information revealing the identity of victims of crime and minors that are victims of sexual assault from disclosure laws. Posting uncensored videos of crime victims is a direct violation of that statute, and violates the first condition of RCW 42.56.050, where this information would likely be highly offensive to a reasonable person. This also holds true for witnesses and undercover police officers, where the disclosure of a person's identity could place that individual in danger of serious harm. Citizens may request that the record be sealed, but the speed of disclosure has a strong chance of overtaking the speed of the request, which also assumes that the citizen is aware of the process.

Another area of significant concern stems from security footage recorded in classrooms, school campuses, and public transportation facilities. It can only record video images and not sound due to state law prohibiting recording conversations, but by definition, this video content is public record. While there may be additional factors such as FERPA regulations that prevent a school security video from being

[ix] See Washington State RCW 9.73.030

released,[7] the fact of the matter is that minors and other protected groups are being recorded, and the images are available to the public.

### Permanence of the Internet

Before the widespread use of the Internet, the life of a record was based on the medium that it was held in. Electronic and paper records and other mediums last until destroyed or degraded. The same phenomenon holds true for modern public records, even if stored electronically. The possible expiration of data granted a degree of control over the information over time, creating advantages and disadvantages for both personal privacy and government transparency.

The Internet has fundamentally changed this principle. Once a data element has been published to the Internet, all control over the data disappears. Links can be removed and search algorithms modified, but the content is permanently released. The data science industry has created (and will continue to create) mechanisms for finding, indexing, and analyzing data at ever-increasing magnitudes, which, true to the nature of technology[8], only magnifies the privacy problems presented with collecting public image data.

### "…highly offensive to a reasonable person…"

As discussed before, collecting data is a good thing. An image taken for a publicly oriented data-driven purpose is generally unobtrusive. It is not the single element that is the problem. It is the presence and cataloguing of many elements in relation to each other that create a whole greater than the sum of its parts. Public image data is enabling private and public sector agents to reach further than intended and approved.

Re-use of image data by government agencies is perhaps a greater cause for concern than how citizens or the private sector might use the same data. Baase raises the question of what government security forces may do with facial recognition software and the host of images available for analysis.[9] As Baase mentions, uncensored access to raw image data allows for easy monitoring of journalists, political dissidents, and to reflect a recent issue, suspected radical Moslems. While citizens have a legal claim to request information on these activities, the public may not be aware that these activities are occurring in the first place. Regardless of what the data is being used for, the fact remains that collateral data is usable by whoever holds it. As far as Washington State is concerned, there seems to be a distinct lack of legislation guiding

the use or re-use of image data, except for traffic camera images that have distinct usage guidelines[x].

Public image data also has significant implications to the private sector. Most agencies have restrictions on private sector companies requesting public data[xi] to protect privacy. The ability to safeguard public data from being used by private entities stops when the data is published to the Internet. Google has made its mark on mapping applications but has had to do so by driving around and taking pictures of public spaces. Should a citizen request image data and post it online, there is nothing preventing Google from using the image and its metadata since it is now in a public space.

### "…of general interest"

The presumption of innocence[xii] is a cornerstone of the American justice system, yet posting the uncensored footage of an arrest will do less to uphold that principle with the general public. What would happen if a man were arrested under suspicion child molestation? Even if he was acquitted later, how likely is it that he would have no negative repercussions in his community or in his career? In this situation, the suspect could easily be outraged by the release of the video footage, but what is the definition of what is "of interest" and "not of interest" to the general public? We can argue that, since communities approve both the laws that govern behavior and empower government agents to uphold those laws, that there is a justifiable interest in knowing about those that violate those laws.

We have seen with such incidents such as "tippergate" in Seattle of October 2011[10] that the general public can react quickly, negatively, and in some cases, violently to incidents not only between public agents and citizens but also between citizen and citizen. In the case of police video, there can be any number of situations where mass public reaction does more damage than the incident itself. Granted, a large-scale public reaction is unlikely to occur for every arrest, but damage done by one individual is still damage and it can still be just as devastating. Juvenile criminals also face an additional complication. Uncensored video would prevent a record from ever being completely sealed and discloses the identity of a minor that falls into the "of interest" category to society, even though society has chosen to protect this class of citizen.

---

[x] See Washington State RCW 46.63 for more information

[xi] A specific statute in Washington State law regarding this issue was not found.

[xii] Definition of the presumption of innocence can be found at http://www.law.cornell.edu/wex/presumption_of_innocence

The records mentioned in this section have always been available, and the problems discussed have not happened at a nationally recognized scale. The key difference is that these records are now being posted to the Internet, and once the data is there, it can never be retracted. An argument could easily be made that an extreme criminals such as murderer or rapist has forfeited all rights to have information about his case controlled. The argument starts to weaken as the severity of the crime is lessened and as cases become more complex. Is it just for a person with a DUI from twenty years ago to have his image posted along with recent DUI offenders? What about the person who was given a traffic ticket for going 10 miles per hour over the speed limit? Does the position of a death row inmate change from criminal to victim if he is acquitted of his crime?

The measure of justice must be equitable to the measure of the crime. Posting uncensored video of every criminal incident to the Internet inhibits a sentence from ending, inhibiting a former criminal's ability to engage in the common occupations of life[11] once his dues to society have been paid. Uncensored image and video generates a higher cost to privacy and the well-being of our communities than the benefit gained for transparency.

**Policy Alternatives**

The fact that current policy does not address current privacy issues is a tired subject, but little actual progress has been made to date. President Obama's Consumer Privacy Bill of Rights[xiii] is the most significant legislation designed to protect privacy, but the legislation is focused on private companies collecting consumer information. In order for the legislation to be effective, it needs to have explicit mandates for government to manage data is the same way as private companies. Even so, this particular legislative piece is still just a proposal to Congress, and the problem of disclosing public data and the risks it poses to privacy is a problem *today*.

The first critical policy change that must be made is to informed consent. Informed consent requires that the use and re-use of the data being gathered be disclosed and to allow the option to opt out. Informed consent will not be necessary for gathering publicly available data gathered in a public place

Part of the policy issue stems from two different problems being assessed in isolation. The first problem is

[xiii] The full text of the Consumer Privacy Bill of Rights is available at the following link: http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

that of collecting data; public agencies have a need to collect data in order to maintain and improve society. The second problem is that of privacy; citizens have a right to know what information the government collects and to keep sensitive information contained. If addressed in isolation, the best solution for each of these problems is the worst outcome for the other. If the problems were to be combined, the requirements of each issue may be re-stated as constraints for the solution. Rather than relying solely on image data, as it exists today, policies could be supplemented with the condition that the method of collecting data must be designed to optimize the collection of the target data and to minimize to collection of collateral data to the fullest extent that technology allows. Changing the assumption that images and video are the only medium for collecting data can open up a world of possibilities.

Images may not be necessary at all in the case of utilities data such as traffic flow and parking utilization. When I was younger, I worked for the City of Everett transportation department. One of the common traffic data collection devices were simple rubber tubes stretched across a road. These tubes were connected to a small box that would record the air pressure when a car or truck drove over the tubes. By analyzing the velocity of air and timing between airbursts, the engineers could determine the gross weight, axle count and dimensions, and speed of a vehicle along with the total count of vehicles that passed that spot throughout a period of time. Such a simple device collected highly usable data without compromising privacy. What innovations might spring up if the focus shifts to collecting the greatest amount of data on traffic movement and parking utilization *without* collecting personally identifiable information?

The same principle applies to body-mounted police video. The intent of the technology is to monitor the behavior of the police officer, not to broadcast sensitive information about citizens. To be fair, video appears to be the most effective method given current technology, but how the data is both recorded and disclosed to the public could be improved in light of a new policy. As an active agent of the government a police officer's conduct is subject to scrutiny, so none of the current situation would need to change; video of an officer's conduct should still be uncensored to the public. However, the citizens in the video have a right to privacy unless the video content is deemed to be of interest to the public. As such, the video content should be anonymized upon recording, to be de-anonymized upon the receipt of a court order during the investigation of a complaint or criminal case. The result would be publicly available video of interactions between police officers and citizens, (possibly with the badge number or police officer's name on the video along with a time and date stamp) without risking the identity of the involved citizen.

A similar concept is loosely captured in section 6, *Focused Collection*, of the Consumer Protection Bill of Rights, but the wording still leaves organizations open to the most convenient data collection method. Policies should focus on encouraging alternative methods of collecting data that minimize or altogether avoid collateral data. For smaller government offices, the issue of research and development resources comes to the forefront against this argument, but this can be avoided by providing funding for citizens or companies to invent solutions. What would happen if student loans were forgiven or there were new tax credits issued in exchange for coming up with a solution to a data-collection problem that did not create a privacy issue?

Content considered "of general interest" to the public also must be more clearly defined. Video and images of citizens involved in legal issues, either as victims or as criminals, have far-reaching consequences for those involved when released to the Internet. The permanent nature of online content should move policy to more robust informed consent procedures or re-structuring the way that data is disclosed.

## Closing

In the Information Age, informed consent is the keystone around which privacy protection is built and is essential to protecting society's sense of privacy. The issue is not with government agents collecting public images. Taking pictures or video (not audio) of things going on in a public place is legal. In fact, it is a core tenant of the First Amendment[xiv]. The issue is that the use of images and video to collect information on traffic patterns, police officer behavior, school security cameras, and other elements generates *collateral data* that can be re-used by government agents, private sector businesses, and individual citizens for purposes outside of its original intent. Informed consent is sorely missing in the management of government image data, and as such is creating multiple avenues for privacy violations. Significant policy changes are needed immediately, before major harm can be done.

What should *not* change, however, is public disclosure policy. The disclosure of public records is critical to a healthy democratic society. Washington State in particular has done what appears to be a good job defining legislation in favor of government transparency. The change in policy should be aimed at minimizing collateral data and optimizing the collection of target. Funding or incentives should support

[xiv] More information on the first amendment http://www.firstamendmentcenter.org/

these new policies such that the cause of the problem is involved in creating the solution.

## References

[1] Baase, Sara. "Chapter 2: Privacy." *A Gift of Fire: Social, Legal, and Ethical Issues for Computing and the Internet*. 3rd ed. Upper Saddle River, NJ: Pearson Prentice Hall, 2008.

[2] Stewart, Darin L. *Building Enterprise Taxonomies*. United States: Mokita, 2008. Print.

[3] Anthony, Sebastian. "Facebook's Facial Recognition Software Is Now as Accurate as the Human Brain, but What Now?" *ExtremeTech*. 19 Mar. 2014. Accessed Nov. 2014 <www.extremetech.com>.

[4] Elinson, Zusha. "Punishment of Police Under Scrutiny." *The Wall Street Journal*. 28 Nov. 2014. Accessed Nov. 2014 <http://online.wsj.com>.

[5] Mapes, Lynda. "Police-shooting Victim 'Struggled with a Lot of Things'" *The Seattle Times*. 1 Sept. 2010. Accessed Nov. 2014 <http://seattletimes.com>.

[6] Mims, Christopher. "What Happens When Police Officers Wear Body Cameras." *The Wall Street Journal*. 18 Aug. 2014. Accessed Nov. 2014 <http://online.wsj.com>.

[7] Steketee, Amy. "The Legal Implications of Surveillance Cameras." *District Administration Magazine*. 1 Feb. 2012. Accessed Nov. 2014 <http://www.districtadministration.com>.

[8] Toyama, Kentaro. "Can Technology End Poverty?" *Boston Review*. 1 Nov. 2010. Accessed Nov. 2014 <http://www.bostonreview.net>.

[9] Baase, Sara.

[10] Kindelan, Katie. "Seattle Waitress Exposes Rude Tipper Online, Nabs Wrong Guy." *ABC News*.13 Oct. 2011. Accessed Nov. 2014 <http://abcnews.go.com>.

[11] "The Right of Privacy: Is It Protected by the Constitution?" Exploring Constitutional Conflicts. Project of the University of Missouri-Kansas City School of Law. Accessed Nov. 2014 <http://law2.umkc.edu>.