Surveillance, privacy and the ethics of vehicle safety communication technologies

M. Zimmer[1]
PhD Candidate, Department of Culture and Communication, New York University
East Building, 239 Greene Street, 7th Floor, New York, NY, USA 10003
T: 212-998-5191; F: 212-995-4046; E: mtz206@nyu.edu

Abstract

Recent advances in wireless technologies have led to the development of intelligent, in-vehicle safety applications designed to share information about the actions of nearby vehicles, potential road hazards, and ultimately predict dangerous scenarios or imminent collisions. These vehicle safety communication (VSC) technologies rely on the creation of autonomous, self-organizing, wireless communication networks connecting vehicles with roadside infrastructure and with each other. As the technical standards and communication protocols for VSC technologies are still being developed, certain ethical implications of these new information technologies emerge: Coupled with the predicted safety benefits of VSC applications is a potential rise in the ability to surveil a driver engaging in her everyday activities on the public roads. This paper will explore how the introduction of VSC technologies might disrupt the 'contextual integrity' of personal information flows in the context of highway travel and threaten one's 'privacy in public.' Since VSC technologies and their related protocols and standards are still in the developmental stage, the paper will conclude by revealing how close attention to the ethical implications of the remaining design decisions can inform and guide designers of VSC technologies to create innovate safety applications that increase public safety, but without compromising the value of one's privacy in public.

Keywords: surveillance, privacy, contextual integrity, value sensitive design, vehicle safety communication technology

INTRODUCTION

Imagine approaching a curve and having a roadside sign tell your car the optimal speed for safe navigation, and your car informing you if you are going too fast. Imagine your car warning you to begin braking because the traffic light you are approaching will be red by the time you reach the intersection. Imagine that same traffic light receiving messages from other nearby cars so it can warn you if another vehicle is likely to run a red light. Imagine a car in front of you, but out of your view,

[1] This work was supported by the National Science Foundation PORTIA Grant No. CNS-0331542, and could not have been completed without the valuable guidance of Prof. Helen Nissenbaum (New York University) and Prof. Dan Boneh (Stanford University). I am grateful to many other colleagues who generously contributed to this work with excellent comments and suggestions, including Emily Clark and Steve Tengler at the VSCC, and Sam Howard-Spink, Joseph Reagle and Tim Weber at New York University. Drafts were further sharpened through opportunities to present at colloquia and conferences sponsored by New York Unviersity's Department of Culture & Communication, the American Association for the Advancement of Science, the Society for Philosophy and Technology, and Computer Ethics: Philosophical Enquiry.

communicating with your car so if it suddenly stops, you will be warned before you can see what has happened. These are but some the potential *safety benefits* of new vehicle safety communication technologies.

Now, imagine your car as a node in a wireless network, constantly making connections and communicating with other nearby cars and roadside infrastructure. Imagine your car openly transmitting its location, speed, and identity 10 times per second, every second your car is on, receivable by anyone within 1000 meters. And instead of your car needing to be - by chance - in clear view of traffic cameras or law enforcement to be surveilled, imagine the ability to set up a wide-range data receiver to electronically surveil and record the message activity of every single car that passes within a half-mile radius. These are but some of the potential *surveillance threats* of new vehicle safety communication technologies.

Recent advances in wireless data communications technologies have led to the development of Vehicle Safety Communication (VSC) applications. This new breed of automotive technologies combines intelligent on-board processing systems with wireless communications for real-time transmission and processing of relevant safety data to provide warnings of hazards, predict dangerous scenarios, and help avoid collisions. While the technical standards and communication protocols for VSC technologies are still being developed, it becomes vital to consider potential value and ethical implications of the design of these new information technologies. Coupled with the predicted safety benefits of VSC applications is a potential rise in the ability to surveil a driver engaging in her everyday activities on the public roads, a unique privacy concern known as the problem of 'privacy in public' (see Nissenbaum, 1998).

Given the ubiquity of information technology in our lives, it is vital to consider what our commitment to such systems means for moral, social and political values, including the value of privacy.[2] By approaching the problem of privacy in public through the theory of 'contextual integrity,' this paper will discuss how the design of VSC technologies might alter personal data flows in political

[2] There has been increasing interest in and concern with the value implications of information technologies, a perspective commonly referred to as 'Values in Technology' or 'Value-Sensitive Design.' This emerging discipline recognizes how information and communication technologies act as a crucial medium for asserting social, political, ethical and moral values. For more information, visit http://www.nyu.edu/projects/valuesindesign/index.html.

ways, contributing to the growing ubiquity of public surveillance and threatening the value of privacy in public. The ultimate goal of the research is to raise awareness within the VSC design community of the critical value and ethical implications of their technical decisions, and to influence the design of VSC technologies so that the value of privacy becomes a constitutive part of the technological design process, not just something retrofitted after completion and deployment.

VEHICLE SAFETY COMMUNICATION TECHNOLOGY

Traffic accidents are often a result of the typical driver's inability to assess quickly and correctly the current and impending driving situations. Too often, a driver has incomplete information about the status of traffic signals, road conditions, or the speed and location of nearby vehicles, and is forced to make operating decisions, such as when to brake or change lanes, without the benefit of all available data. In an attempt to alleviate the problem of incomplete information, the U.S. Department of Transportation launched the Vehicle Infrastructure Integration (VII) initiative, with the goal of achieving a 'nationwide deployment of a communications infrastructure on the roadways and in all production vehicles and to enable a number of key safety and operational services that would take advantage of this capability' (U.S. Department of Transportation).[4]

A key VII initiative is the development of Vehicle Safety Communication (VSC) technologies, intelligent on-board safety applications that share, receive and process data from the surrounding environment. Made possible by recent advances in wireless data communication technology, VSC solutions aim to provide the driver every possible opportunity to avoid an accident, including providing real-time information about the surrounding road conditions as well as nearby vehicles, warnings of hazards, and prediction of dangerous scenarios or imminent collisions.

Vehicle safety applications rely on the creation of autonomous, self-organizing, point-to-multipoint wireless communication networks - so-called ad-hoc networks - connecting vehicles with roadside infrastructure and with each other. In these networks, both vehicles and infrastructure collect local data

[4] More historical details can be found in Glancy (1995, p. 151, at note 3).

from their immediate surroundings, process this information and exchange it with other networked vehicles to provide real-time safety information about the immediate surroundings. Data messages, which are transmitted by your car 10 times per second, potentially include your car's location, time and date stamps, vehicle speed & telemetry data, and some sort of vehicle or message identification number.

While over 75 potential uses of VSC technology have been envisioned, current development has focused on 8 core safety applications:

- *Traffic Signal Violation Warning*: uses infrastructure-to-vehicle communication to warn the driver to stop at the legally prescribed location if the traffic signal indicates a stop and it is predicted that the driver will be in violation.
- *Curve Speed Warning*: aids the driver in negotiating curves at appropriate speeds.
- *Emergency Electronic Brake Lights*: when a vehicle brakes hard, the Emergency Electronic Brake light application sends a message to other vehicles following behind.
- *Pre-Crash Warning*: pre-crash sensing can be used to prepare for imminent, unavoidable collisions.
- *Cooperative Forward Collision Warning*: aids the driver in avoiding or mitigating collisions with the rear end of vehicles in the forward path of travel through driver notification or warning of the impending collision.
- *Left Turn Assistant:* provides information to drivers about oncoming traffic to help them make a left turn at a signalized intersection without a phasing left turn arrow.
- *Lane Change Warning*: provides a warning to the driver if an intended lane change may cause a crash with a nearby vehicle.
- *Stop Sign Movement Assistance*: provides a warning to a vehicle that is about to cross through an intersection after having stopped at a stop sign.

To help facilitate the advancement of these VSC applications, seven major auto manufactures have formed a cooperative research program called the Vehicle Safety Communications Consortium (VSCC).[5] The main objectives of the VSCC are to identify and evaluate the safety benefits of vehicle safety communication applications, and estimate their deployment feasibility; assess the associated communication and data requirements specific for VSC applications; investigate any issues that might

[5] VSC Consortium members are: BMW, DaimlerChrysler, Ford, General Motors, Nissan, Toyota, and Volkswagen.

affect the successful deployment of vehicle safety applications; and contribute to the formation of the necessary technical standards and communication protocols.

As of the writing of this paper, communications security remains an 'open issue' for VSC applications (see Vehicle Safety Communications Consortium, pp. 5, 138). Primary security concerns include assuring that transmissions are generated by a trusted source (*data authenticity*), and that the data has not been degraded or tampered with after it was generated (*data integrity*). For example, with the Traffic Signal Violation Warning application, the in-vehicle system will use information communicated from the infrastructure located at traffic signals to determine if a warning should be given to the driver. An incorrect transmission from a malfunctioning, invalid or compromised unit might jeopardize the safety of the vehicle and endanger others in the vicinity. Similarly, future implementation of safety applications (such as the Approaching Emergency Vehicle Warning application) would be greatly compromised without assurance that transmissions are from an authentic source (in this case, from an actual emergency vehicle).

Along with the need for authenticity and integrity in VSC data communications, *data anonymity* has also emerged as key security issue. Since the safety messages that originate from end-user vehicles and could potentially contain identifiable data, the VSCC has established the requirement that the design of the system should make it difficult to identify the source of these transmissions. From the VSCC's perspective, this requirement is necessary to 'ally consumer fears that the system might be used to build tracking mechanisms that would allow harassment, automatically issue speeding tickets, or otherwise behave in an undesirable way' (NTRU, 2004, p. 31). Recent work by Stanford computer scientist Dan Boneh has attempted to address the VSCC's technical requirements to ensure secure, reliable, and privacy-protecting encryption of the personal information flows envisioned by VSC technologies (Boneh, Boyen, and Shacham, 2004). Yet, at the time of this writing, Boneh's recommendations have yet to be integrated into the design standards and protocols of VSC technology. In fact, conversations with some of the members of the VSCC reveal that while this design community has recognized the importance of addressing data anonymity, issues concerning a driver's *privacy*

remain either misunderstood or under-conceptualized, and privacy-protecting measures, such as Boneh's, remain largely underutilized.

It becomes vital, then, for the designers of these new safety applications to understand fully how the design of VSC technologies might alter personal information flows in politically and ethically significant ways. Coupled with the predicted safety benefits of VSC applications is a potential rise in the ability to surveil people engaging in their everyday activities on the public roads. For privacy theorists, this concern has been labeled the problem of 'privacy in public.' As the remainder of this paper will argue, approaching the problem of privacy in public through Nissenbaum's theory of 'contextual integrity' reveals how the design of VSC technologies might significantly alter the flow of personal information in the context of highway travel, contributing to the growing ubiquity of public surveillance, and threatening the value of privacy in public.

UNDERSTANDING PRIVACY AS 'CONTEXTUAL INTEGRITY'

Privacy in Public

Public surveillance has become a part of a modern citizen's everyday life. Along with the ubiquitous presence of surveillance cameras along our streets, in front of our buildings and inside our public parks, interactions with health care providers, online retailers, highway tollbooths, local grocery stores and libraries result in the collection, analysis, storage and sharing of information about one's address, purchasing habits, age, education, health status, travel activity, employment history, phone numbers and much more. Information technology plays a vital and unmistakable role in the massive amount of personal information being collected: frequent shopping cards connect purchasing patterns to customer databases, radio frequency identification (RFID) tags on dashboards enable the recording and billing of vehicles passing through highway tollbooths, Internet cookies surreptitiously track website traffic and usage, and encoded employee ID cards manage access to locations while creating a record of one's

movements. Recent advances in digital networking, data storage capacity and processing power have enabled previously unimaginable levels of interconnectivity, aggregation, and real-time analysis of a wide array of personal information. Without information technology, the gatherers and users of information would not be able to collect, analyze, store or share information with such ease.

The growing ease of collecting personal information has not gone unnoticed. Privacy scholars have attempted to contextualize these practices of public surveillance and information aggregation within existing legal and philosophical conceptualizations of privacy, struggling with how to build a theory of 'privacy in public' (see Allen, 1988; Nissenbaum 1997, 1998; Slobogin, 2002). Yet, as Nissenbaum (1998) has noted, many theories of privacy fall short of properly addressing the problem of privacy in public, either dismissing it or ignoring it altogether. She cites three factors that contribute to the general disregard of privacy in public. *Conceptually*, the idea that privacy might somehow be violated in public space is often considered paradoxical. For many, the value of privacy applies to an individual's private sphere alone. Such thinking follows the lines of a private/public dichotomy, marking distinct realms of sensitive (private) information, on the one hand, and the nonsensitive (public) information, on the other. In this sense, one's right to privacy is situated as a method of keeping government out of the private lives of individuals; the right to privacy is an argument for protection of intimate and sensitive information against government intrusion. In such a conceptualization, the government has no right to the sensitive (private) information of what goes in one's bedroom, but has the right to the nonsensitive (public) information of what tollbooth one's car passes through. In short, driving one's car is considered a public act, and collecting one's license plate number (which is displayed in full public view) would not consist of an intrusion into sensitive information.

A second factor contributing to the dismissal of privacy in public is *normative* in nature. Normative arguments for the preservation of privacy recognize that privacy, as an important value and interest, must be balanced against other, competing interests. A simple example of such normative judgment is our willingness to relinquish personal privacy and allow our luggage to be searched in airports: safety and security are judged more important in such situations when balanced against personal privacy.

Similar balancing often threatens any concern for privacy in public. Since much of the personal information collected in situations of public surveillance are considered innocuous, it is easy for other, competing interests to outweigh the need to keep such information private. For example, the items purchased by a shopper at the grocery store are, at least in isolation, not considered sensitive or private, so the interests of the grocer to ensure the shelves are properly stocked to maximize both customer satisfaction and his profits prevail.

The third explanation why privacy in public is overlooked recognizes that the *empirical* status of privacy in public has failed to garner proper attention by privacy theorists. Simply put, prior to recent advances in information technology, the problem of privacy in public was not experienced in one's everyday life to the extent it is today. In the past, most people reasonably assumed that their day-to-day movements and activities were neither being surveilled nor cataloged. As Nissenbaum (1998) relates:

> An individual going about his daily activities does not worry about undue surveillance even if he is observed by one person, on April 4, 1997, to be wearing chinos, a blue polo shirt and loafers and to be tall and blond. By another, he is observed purchasing three cases of wine from the local liquor store. By a third he is overheard discussing his son's progress with his school teacher. Later that day, by a fourth, is observed participating in a march for gay and lesbian rights. All these activities occur in the public all; all may be observed, even noted. No single one of these instances of being observed is necessarily threatening or intrusive. (p. 576)

In examples such as this, no general or systematic threat to privacy in public is evident; people have come to count on virtual anonymity as they engage in their daily, public activities. From an empirical sense, the problem of privacy in public was not compelling enough to garner signification attention by privacy theorists.

However, developments in information technology challenge the conceptual, normative and empirical explanations for the lack of attention given to the problem of privacy in public. These developments include the ability to transmit and share large amounts of information across global digital networks, the ability to aggregate disparate sets of information into large databases, reductions in the cost of data storage to facilitate such databases, and the increase in processing power to ease the processing and analysis of data. Such advancements in information technology mean that there is virtually no limit to the amount of information that can be recorded, virtually no limit to the level of

data analysis that can be performed, that the information can be shared with ease, and virtually stored forever. The consequence of the emergence of such powerful information technology is a rise in the magnitude, detail, thoroughness and scope of the ability to surveil everyday people engaging in their everyday, public activities.

The problem of privacy in public, then, emerges as a very important concern for the protection of personal information. Privacy laws and theories have not kept up with issues that have developed in the wake of advanced uses of information technology, and the problem of privacy in public is a key casualty of this oversight. Considering the conceptual, normative and empirical reasons noted above, existing theories lack, in Nissenbaum's words, 'the mechanisms to deal with conflicts involving privacy in public and have generally not taken up hard questions about surveillance in non-intimate realms to determine when such surveillance is morally acceptable and when not' (1998, p. 579). In response to the general ambivalence to the problem of privacy in public by existing legal and theoretical approaches to privacy, Nissenbaum suggests a new conceptualization of privacy as 'contextual integrity.'

Privacy as Contextual Integrity

'Privacy as contextual integrity' is not a full theory of privacy; rather, it is a benchmark theory, a conceptual framework that links the protection of personal information to the norms of specific contexts. Rejecting the broadly defined public/private dichotomy noted above, contextual integrity recognizes that all of the activities people engage in take place in a 'plurality of distinct realms':

> They are at home with families, they go to work, they seek medical care, visit friends, consult with psychiatrists, talk with lawyers, go to the bank, attend religious services, vote, shop, and more. Each of these sphere, realms, or contexts involves, indeed may even be defined by, a distinct set of norms, which governs its various aspects such as roles, expectations, actions, and practices. (Nissenbaum, 2004, p. 137)

Within each of these contexts, norms exist - either implicitly or explicitly - which both shape and limit our roles, behaviors and expectations. For example, it might be acceptable for me to approach a stranger and offer her a hug at a moving religious service, but not in the grocery store. A judge willingly accepts birthday gifts from co-workers, but would hesitate to accept one from a lawyer

currently arguing a case in her courtroom. It is deemed appropriate for a physician to ask me my age, but not for a bank teller. While it is necessary for an airline to know my destination city, it would be inappropriate for them to ask where I will be staying, whom I will be meeting with, or what will be discussed.

In short, norms of behavior vary based on the particular context. The latter examples above reveal the ways in which norms govern the flow of *personal information* in particular contexts. Whether in discussions with a physician, purchasing items in a store, or simply walking through a public park, norms of information flow govern what type and how much personal information is relevant and appropriate to be shared with others. The theory of contextual integrity is built around the notion that there are 'no arenas of life *not* governed by *norms of information flow*' (Nissenbaum, 2004, p. 137). My being in a public place does not imply that 'anything goes' in terms of my personal information. To illustrate this point, Nissenbaum outlines two types of informational norms in her theory of contextual integrity: norms of appropriateness, and norms of distribution.

Norms of Appropriateness

Within any given context, norms of appropriateness distinguish between personal information that is appropriate to divulge and information deemed inappropriate. Norms of appropriateness 'circumscribe the type or nature of information about various individuals that, within a given context, is allowable, expected, or even demanded to be revealed' (Nissenbaum, 2004, p. 138). In medical contexts, for example, it is appropriate to share details of my personal physical condition, but not my salary or investment portfolio. The opposite is true in the context of meeting with my financial advisor. Even in the most public places, norms of appropriateness apply: it remains in appropriate to ask someone standing among the bustle of Times Square their name. In some contexts, norms of appropriateness are very open, such as in a personal friendship where personal information tends to flow freely. In other contexts, such as the job interview or classroom, more explicit and restrictive norms of appropriateness prevail, and the flow of appropriate personal information is more highly regulated. Nevertheless,

norms of appropriateness apply in all situations: among both strangers and loved ones, in personal and professional interactions, in private and public.

Norms of Distribution

In addition to appropriateness, the distribution of personal information is also governed by norms in any given context. As noted above, the norms of appropriateness might be relatively open in the context of a personal friendship: the minutiae of my everyday activities are freely shared, my political opinions, my emotions, perhaps even my sexual history. This openness in norms of appropriateness does not imply equally open norms of flow or distribution. While such personal information is considered appropriate to be shared within the context of a friendship, more restrictive norms of distribution prevent my friend from distributing my personal information to a third person. Similarly, norms of distribution allow my physician to share only some of my personal information with other doctors: she might share my symptoms or family history to aid in diagnosis, but not my name. More restrictive norms have been codified into our legal systems, such as the burden necessary for law enforcement to obtain my detail phone records. In such cases, norms protect open distribution of my personal information unless certain requirements are met. Just as with norms of appropriateness, all of our interactions rely on norms of distribution to govern how personal information is shared within any given context.

Maintaining Contextual Integrity

The 'contextual integrity' of the flow of personal information is maintained when both the norms of appropriateness and the norms of flow are respected. Conversely, if either norm is violated in a particular context, the contextual integrity of the flow of personal information is violated. Contextual integrity, then, is a benchmark theory of privacy where claims of a breach of privacy are sound only in the event that one or the other types of informational norms have been violated. Rather than aspiring to universal prescriptions for privacy in public, contextual integrity works from within the normative bounds of a particular context. It is designed to consider how the introduction of a new practice or

technology *into a given context* might impact the governing norms of appropriateness and distribution to see whether and in what ways either of the norms is breached.

A breach of the contextual integrity of information flow in a particular context often triggers an assessment in terms of countervailing values. The preservation of contextual integrity is meant to promote the preservation of privacy of personal information in support of broader social, political and moral values such (1) prevention of information-based harm, (2) autonomy, (3) freedom, and other human values. By disrupting the existing contextual integrity, a new practice or technology might support countervailing values such as (1) freedom of speech, (2) efficiency, or (3) security. When such values clash - when contextual integrity is threatened - it becomes necessary to pursue trade-offs and balance: the practice or technology threatening contextual integrity are either resisted as too invasive as to the privacy of personal information, or the existing norms of information flow are shifted to allow for the new practice or technology. To help illustrate this, we can consider the existing contextual integrity of the flow of personal information in the context of highway travel, and examine how these governing norms might shift with the introduction of new transportation technologies.

CONTEXTUAL INTEGRITY IN HIGHWAY TRAVEL

One of the key ways contextual integrity differs from other theoretical approaches to privacy is that it recognizes a richer, more comprehensive set of relevant, contextual parameters. When considering how the introduction of VSC technologies might mark a significant change in the privacy of one's personal information, the theory contextual integrity forces us to look beyond simple public/private dichotomies and instead consider how the current norms of information flow might be violated. To determine the potential impact of new transportation technologies on the contextual integrity of personal information flow in the context of highway travel, the first step is to understand the existing norms of appropriateness and flow within this particular context.

Existing Norms of Appropriateness in Highway Travel

Most everywhere we drive, we drive in the public world; we are subject to public observation. The disclosure of certain personal information has become normalized in our frequent acts of driving along public roads. With the exception of tinted windows, the occupants of vehicles are observable. While not fully identifiable, occupants can be seen and generally described as male or female, young or old, wearing a suit or a t-shirt, and so on. The norms of appropriateness, then, include visually-observable and generally-identifiable information about a car's occupants, but not specific information such as their names, ages or home addresses.

The identity of the car itself is also governed by norms of appropriateness. Our society celebrates uniqueness and choice in consumer products, and our vehicles reflect these values. As a result, cars of different makes, models, styles, and colors fill the streets. This allows a general level of identifiably of a vehicle: I can observe a green Toyota SUV leave a parking lot and watch it as it navigates through downtown traffic. This simple method of surveillance would not be possible if all our vehicles looked exactly alike, and norms in our culture make it acceptable that others can visually pick out and observe my vehicle. From such simple visual surveillance, others (including law enforcement) can observe what direction I am traveling, approximate my speed, gauge whether or not I am driving recklessly, and so on.

Norms of appropriateness govern an even more efficient method of identifying vehicles: the public display of license plates. Every vehicle on the highway has a unique and visible identifier that, when queried against the proper database, reveals the registered owner of that vehicle.[10] The norms in our society dictate that it is required to display such identifiable information, and that it is appropriate for others to be able to observe, and perhaps even record, this information. The Vehicle Identification Number (VIN), another unique identifier, is also openly displayed, but requires a much closer inspection of the vehicle: it is usually stamped on a small piece of metal near the windshield and not observable from a distance.

[10] Access to such databases is discussed below in relation to norms of flow or distribution.

Norms of appropriateness, then, anticipate the sharing of some generally-observable information: nonidentifiable information about a vehicle's occupants, the type of vehicle, observable information about where the vehicle is going, and the vehicle's license number. Equally important for our discussion is what is *not* appropriate information to be shared: a vehicle's occupants are not expected to share their specific identity within anyone observing them, their exact destination or route, previous location, and so on. Existing norms of appropriateness have deemed it unnecessary to display or share publicly this particular information.

Existing Norms of Distribution in Highway Travel

It is important to note that the norms of appropriateness described above generally deal with visually observable information. The occupants of a vehicle and its license plate number have been deemed appropriate information to divulge, but mainly in visual contexts, and generally in person and in close proximity. Quite simply, someone has to be nearby, watching your vehicle in order to obtain this identifiable information. Considered in relation to norms of distribution, the flow of such identifiable information is generally confined to the likelihood that a person happens to be located in a particular spot in order to observe another vehicle. Further, that person would be unable to observe *all* vehicles and must selectively choose which to examine more closely to determine its occupants, type or license number. It also is unlikely that any one observer would be able to maintain complete surveillance of a particular vehicle as it travels through chaotic rush hour traffic or travels hundreds of miles across country. Such conditions represent natural barriers to mass surveillance of highway traffic, barriers that constitute part of the existing norms of distribution.

Other elements of the norms of distribution in the context of highway travel include legal barriers to the free flow of personal information. While norms of appropriateness allow open access to a vehicles license plate number or VIN, the prevailing norms of distribution restrict the ability to obtain more detailed information based on these unique identifiers. Legal barriers, such as the Drivers' Privacy Protection Act of 1993 reflect the restrictive norms on sharing some personal information to third

parties.[11] For example, a marketing company is prohibited from obtaining a list of all owners of minivans, or a private investigator cannot obtain the name of the owner of a car with a particular license plate number. Other norms of distribution might actually *compel* the sharing of personal information, such as when a police officer has just cause to query a license place number through a database to determine if a car has been stolen. Other norms of distribution ensure, however, that even when we are compelled to provide information, it is used only for the intended purpose and not shared with others.

Shifting Norms with New Transportation Technologies

The norms of appropriateness and distribution noted above represent the general set of norms of information flow in the context of highway travel. Yet, with the introduction of new technologies, these norms shift. One example is the increased use of traffic surveillance cameras. Video cameras were introduced to traffic and safety management systems for roadway, intersection and tollbooth surveillance because of their ability to record and transmit images for immediate or future observation and interpretation. The introduction of this technology disrupted the norm of distribution of identifiable information, since the ability to observe a vehicle is no longer limited to those who happen to be physically located in proximity to the vehicle. Norms were further shifted due to the ability for one person (or institution) to surveil multiple cars at multiple locations simultaneously, the ability to store video footage for later review, and duplicate videos for distribution to other parties.

The increased use of electronic toll collection systems throughout the United States, such as E-ZPass, similarly affects the norms of information flow. E-ZPass utilizes radio frequency identification (RFID) tags to transmit identifiable information about the vehicle for toll billing purposes. As with cameras, E-ZPass technology provides a technological means to collect and store information about the presence of a vehicle without the need for a human to happen to be in the proximity.

The shift in norms of information distribution caused by the introduction of traffic cameras and E-ZPass technologies disrupted the contextual integrity of the flow of personal information in the context

[11] 103rd Congress, H.R. 3365.

of highway travel. The general acceptance and growing ubiquity of traffic cameras and E-ZPass systems suggest that perhaps this particular disruption of contextual integrity in the flow of personal information has been tolerable; some other value was deemed more serious or urgent, and the norms of personal information flow were adjusted to accommodate these new technologies into the context of highway travel. In the case of traffic cameras, perhaps the competing value was public safety at dangerous intersections. With E-ZPass, increased efficiency in toll collection might have justified a shift in the existing norms to allow the automatic and electronic transmission of identifiable information from one's car to a central billing authority. It is important to note, however, that the introduction of such technologies, and the apparent shifting of contextual norms of appropriateness and distribution, has not occurred without concern or public debate (see Selingo, 2001; White, 2003).

VSC TECHNOLOGY AND CONTEXTUAL INTEGRITY

The growing use of video traffic cameras and electronic toll systems serve as examples of how the introduction of a new technology impact the contextual integrity of personal information flows in the context of highway travel. Since VSC technology is still in development, its impact on the flow of personal information has not yet been fully contemplated. Given the general ambivalence to the problem of privacy in public noted above, it would not be surprising if VSC technologies fail to spark any significant change in the mechanisms currently in place to deal with conflicts involving privacy in public. When viewed within existing theories of privacy, any potential impact by VSC technologies on the flow of personal information could likely fall victim to the conceptual, normative and empirical shortcomings previously discussed. Following Nissenbaum's prescription, however, it becomes more useful to examine how the introduction of VSC technology would affect the normative standards of information flow for highway travel rather than trying to fit into the universal prescriptions of existing privacy theories. We must consider how the insertion of Vehicle Safety Communication technologies into the context of highway travel might disrupt the existing norms of appropriateness and distribution of personal information.

Potential Impact on Norms of Appropriateness

Existing norms of appropriateness in the context of highway travel anticipate the sharing of some generally observable information: nonidentifiable information about a vehicle's occupants, the type of vehicle, observable information about where the vehicle is going, and the vehicle's license number. The introduction of VSC technology into the context of highway travel might disrupt these norms of appropriateness for the sharing of personal information. Applications such as the Pre-Crash Sensing for Cooperative Collision Mitigation require the transmission of a vehicle's specific location (GPS coordinates) to help prevent impending collisions. Currently, third parties can visually-observe that a vehicle is 'in Times Square,' but with the implementation of VSC technology, they might know the vehicles precise location, '40.75704, -73.98597.' VSC technologies might also increase the accuracy of vehicle identification. Just as all vehicles openly display their unique license number, VSC technologies might also transmit a unique identifier. But while both represent the disclosure of identifiable information, the precision of the transmitted data with VSC technology eliminates the uncertainty of whether an observer visually read the license plate number correctly (whether they had a clear view or if weather conditions were a factor). The added precision and accuracy of a transmitted identification number enabled by VSC technology upsets the current norm of only appropriate visual and nonspecific information.

The precision of information regarding a driver's habits and current status also increases with the introduction of VSC technology. The Pre-Crash Sensing application, for example, will process the telemetry of the both the driver's vehicle and any oncoming vehicle. Such specific data includes vehicle speed, acceleration (longitudinal, lateral and vertical), heading, yaw-rate, brake position, throttle position and steering wheel angle. Today, without such VSC technologies, observers can only visually estimate as to a vehicles speed or operational status.[12] With the introduction of VSC technology, the range of precise information made available about a vehicle's performance could potentially disrupt the existing norms of information appropriateness.

[12] One exception being law enforcement who can measure speed more accurately with radar or laser technologies. In some jurisdictions, even this is regulated by legal norms which require posting of 'radar enforced' signage.

Potential Impact on Norms of Distribution

By overcoming some of the natural barriers to mass surveillance of highway traffic, VSC technologies might also disrupt the norms of distribution of personal information. Vehicles equipped with VSC technologies will be constantly transmitting information about their identity, location and status for reception by other vehicles, roadside infrastructure, or anyone else with the proper receiving equipment. Like with traffic cameras, humans no longer need to be positioned in a particular place to visually observe a vehicle; all that is needed is a well-placed receiver and information for all passing vehicles can be recorded. Even more, a series of receivers could collect information from the same vehicle over a span of miles. VSC technology has the potential to disrupt the natural barriers that previously limited the ability to track individual vehicles over space and time. Rather than a single piece of information being observed by a person or camera that just happens to be at the right place at the right time, VSC technologies might allow information to be gathered and consolidated on a large scale and across a large area.

VSC technologies disrupt the norms of distribution further. While existing traffic cameras allow the archival and retrieval of video surveillance images, the digital nature of the information provided by VSC applications vastly expands the ability to process, store and distribute vast amounts of personal information about individual vehicles. The processing of digital information can be done electronically, alleviating the need for a human to physically view hours of camera footage, and increasing exponentially the size and complexity of data analyses. Additionally, the digital nature of vehicle data enabled by VSC technology expands the ability and reduces the cost for distributing information to third parties, potentially including insurance companies, marketers, or other government agencies who might have interest in detailed diver data.

Overall Impact on Contextual Integrity

By approaching the introduction of VSC technologies through the lens of ‘contextual integrity,’ we can see how the design of these systems might alter the flow of personal information in the context of

highway travel and threaten the value of privacy in public. VSC technologies enable the collection of information on where drivers go, when they made their trips, and what routes they used. They represent a shift from drivers sharing only general and visually-observable information to the widespread and constant broadcasting of precise, digital information about their daily activities. With the potential integration of VSC technologies into our daily activities on the public roads, we are in danger of violating the norms of personal information flow in the context of highway travel.

This potential breach of contextual integrity of information flow will prompt the weighing of countervailing social values: will the increase in public safety brought about by these news technologies outweigh the increased surveillance and threat to one's privacy in public? Or will resistance to widespread surveillance on the roads force changes in the design of such technologies? The ubiquity of video traffic cameras and electronic toll systems provide a glimpse of how the introduction of similar technologies have shifted the norms of personal information flow, but when considering VSC applications, it becomes important to remember that these technological systems are *not yet fully developed*. The remaining design decisions of VSC technologies will have significant impact in the balancing of these conflicting values and whether a breach of contextual integrity is accepted or rejected by society.

CONCLUSION

By predicting the impact VSC might have on the contextual integrity of personal information flows in the context of highway travel, this paper has revealed how the design of such technologies implicate the value of privacy. VSC technologies enable a rise in the magnitude, detail, thoroughness and scope of the ability to surveil everyday people engaging in their everyday, public activities. The goal of this research is to raise awareness within the VSC design community of these ethical implications of their design decisions, and to influence the design of VSC technologies so that the value of privacy becomes a constitutive part of the technological design process, not just something retrofitted after completion and deployment. When considering the ramifications of the remaining design decisions for VSC technology, a wide range of potential issues and questions arise: What kind of identifiable information

will be transmitted? Who has access to these data streams? Could transmissions be archived for later retrieval? Can a driver opt to turn off the system? Who owns this information? Will there be limits on its use? Will driving habits (such as speeding, performance on curves, adherence to traffic signals) be collected and made available to insurance companies? Will service providers be able to sell information on a vehicle's common travel patterns to marketers? What level of access will law enforcement or other government agencies enjoy? What restraints will exist? Can auto manufacturers or dealers download personal information from the vehicle's processing computer?

These questions, and countless others like them, remain largely unanswered in the current design stages of VSC technology. VSC engineers need to understand how these design decisions might affect the normative standards of personal information flow in the context of highway travel. It becomes vital, then, to engage directly with the VSC design community to raise awareness of the ethical implications of their design decisions and to make the value of privacy in public a constitutive part of the technological design process, *before* VSC systems are deployed in society. By working alongside the VSC design community through the lens of value-sensitive design,[13] this project can help preserve the value of 'privacy in public' in the design of these transportation technologies. The research supporting this paper, culminating in a set of design heuristics to guide the VSC engineers, will contribute to the development of innovative technologies that increase public safety, while seeking to avoid 'driving to the panopticon' (Reiman, 1995) of widespread surveillance and the further erosion of the value of privacy in public.

[13] The methodology of 'value-sensitive design' has emerged to help researchers identify, understand, anticipate and address the ethical and value-laden concerns that arise from the rapid design and deployment of media and information technologies (see, for example, Friedman, 1999).

REFERENCES

Allen, A. (1988) *Uneasy access: privacy for women in a free society*. Rowman & Littlefield, Totowa, NJ.

Boneh, D., Boyen, X. and Shacham, H. (2004) Short group signatures. *Proceedings of Crypto '04*, LNCS 3152, p. 41-55.

Branscomb, L. and Keller, J. (eds) (1996) *Converging infrastructures: intelligent transportation and the national information infrastructure*. MIT Press, Cambridge, MA.

Friedman, B. (1999) *Value-sensitive design: a research agenda for information technology* (Contract No.: SBR-9729633). National Science Foundation, Arlington, VA; see: http://www.ischool.washington.edu/vsd/.

Garfinkel, S. (1996) Why driver privacy must be a part of ITS. *In*: L. Branscomb and J. Keller (eds) *Converging infrastructures: intelligent transportation and the national information infrastructure*. MIT Press, Cambridge, MA. p. 324-340.

Glancy, D. (1995) Privacy and intelligent transportation technology. *Santa Clara Computer & High Tech Law Journal*, 11, 151-203.

Nissenbaum, H. (1997) Toward an approach to privacy in public: the challenges of information technology. *Ethics and Behavior,* 7 (3), 207-219.

Nissenbaum, H. (1998) Protecting privacy in an information age: the problem with privacy in public. *Law and Philosophy,* 17, 559-596.

Nissenbaum, H. (2004) Privacy as contextual integrity. *Washington Law Review,* 79 (1), 119-157.

NTRU. (2004, June 15) *Consolidated report on the requirements for public safety security in WAVE systems* (Draft 0.8). IEEE.

Reiman, J. (1995) Driving to the panopticon: a philosophical exploration of the risks to privacy posed by the highway technology of the future. *Santa Clara Computer and High Technology Law Journal,* 11 (1), 27-44.

Selingo, J. (2001) It's the cars, not the tires, that squeal. *The New York Times*, October 25, 2001, p. G1, G8.

Slobogin, C. (2002) Public privacy: camera surveillance of public places and the right to anonymity. *Mississippi Law Journal,* 72, 213-299.

U.S. Department of Transportation, *Vehicle Infrastructure Integration (VII): Major initiatives* [online]. Available from http://www.its.dot.gov/initiatives/initiative9.htm [Accessed 18 December 2004].

U.S. Department of Transportation and National Highway Traffic Safety Administration. (2005, Janurary) *Traffic safety facts 2003: a compilation of motor vehicle crash data from the Fatality Analysis Reporting System and the General Estimates System.* Washington, DC: USDOT, (DOT HS 809 775).

Vehicle Safety Communications Consortium. (n.d.) *Vehicle safety communications project: Task 3 final report: identify intelligent vehicle safety applications enabled by DSRC.* Author.

White, J. (2003, Spring) *People not places: a policy framework for analyzing location privacy issues* [online]. Electronic Privacy Information Center. Available from http://www.epic.org/privacy/location/jwhitelocationprivacy.pdf [Accessed 18 February 2005]