PERSONAL INFORMATION AND THE DESIGN OF VEHICLE SAFETY

COMMUNICATION TECHNOLOGIES: AN APPLICATION OF PRIVACY AS

CONTEXTUAL INTEGRITY

Submitted to Science & Technology in Society:
An Interdisciplinary Graduate Student Conference
April 23-24, 2005

Michael T. Zimmer[1]
PhD Candidate, Media Ecology
Department of Culture & Communication
New York University
mtz206@nyu.edu

April 1, 2005

INTRODUCTION

Imagine your car warning you to begin braking because the traffic light your are approaching will be red by the time you reach the intersection. Imagine that same traffic light communicating with your car to warn you that some other vehicle is likely to run the red light. Imagine having the car in front of you tell your car that it is suddenly braking for an emergency, communicating faster than you could see and react to the illumination of its brake lights. These are some the potential *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. Imagine a government agency able to set up an array of data receivers to record the message activity of every single car that passes through a particular neighborhood, or down a particular street leading to a political rally, creating a large database of all vehicle activity. These are some of the potential *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 combine 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. VSC applications rely on the creation of autonomous, self-organizing wireless communication networks – so-called ad-hoc networks – connecting vehicles with roadside infrastructure and with each other. 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 ways that threaten the value of privacy. The ultimate goal of paper is to raise awareness within the VSC design community of the crucial value 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.

VEHICLE SAFETY COMMUNICATION TECHNOLOGY

Before we can ascertain how the design Vehicle Safety Communication technologies might disrupt the existing contextual integrity of personal information flow in highway travel we must first understand the history and context of the technology. As Nissenbaum suggests, it is important to know "who is gathering the information, who is analyzing it, who is disseminating it and to whom, the nature of the information, the relationships among the various parties, and

---

[2] There has been increasing interest in and concern with the value implications of information technologies, a perspective commonly referred to as "Value in Technology." 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.

even larger institutional and social circumstances" (Nissenbaum, 2004, pp. 154-155). A brief history of vehicle safety communications that follows will help us understand the technology's role within a broader effort at ensuring highway safety, and illuminate the various design decisions yet to be made regarding VSC communication and security standards and protocols.

Origins of Intelligent Transportation Systems

Personal mobility is a defining feature of modern American life. Whether commuting from suburbs to urban centers, road-tripping from coast to coast, car-pooling the kids to school or spending a day running errands, Americans demand incredible levels of mobility, primarily secured through the use of private cars. Yet, the very freedom of movement that cars provide is now being threatened by over-burdened transportation systems. Former U.S. Secretary of Transportation Frederica Peña has warned that unless improvements are made to the nation's transportation system, "the projected growth in traffic will increase congestion, reduce mobility, lower business productivity, and adversely affect safety" (Branscomb & Keller, 1996, p. viii). The concern for public safety given the increased use of the nation's transportation system cannot be overestimated. According to the U.S. National Highway Traffic Safety Administration (NHTSA), in 2003 there were an estimated 6.3 million police-reported traffic accidents in the United States, in which nearly 43,000 people were killed and almost 3 million persons injured (U.S. Department of Transportation/National Highway Traffic Safety Administration, 2005). An average of 117 persons died each day in motor vehicle crashes in 2003 – one every 12 minutes. The NHTSA estimates the annual economic impact of traffic-related accidents at over $230 billion.

In response to this evolving crisis, numerous strategies have been implemented to balance the increasing demand for increased mobility with the need to ensure the safe and efficient operation of our highway systems, including government subsidies for public transportation systems, investment in large road construction projects, and an increased commitment to a wide range of technological solutions. An example of this last strategy is the Intelligent Transportation Systems (ITS) program at the U.S. Department of Transportation.[3] Recognizing that the ability to gather, process, analyze, and disseminate information to travelers about the condition and performance of the transportation system is crucial to any attempt to improve system efficiency and safety, the ITS program manages numerous initiatives to add information technology to both our nation's transport infrastructure and vehicles. ITS technologies integrate advanced communications, computers, sensors, satellites, and other information processing technologies into transportation systems, facilitating the collection, processing, and integration of information. By offering real-time information about current traffic conditions, collision-avoidance assistance, automatic emergency incident notification, or vision enhancement systems, ITS solutions aim to help drivers to make better informed, more coordinated, and more intelligent decisions, increasing the overall safety and efficiency of the national highway system.

A key ITS initiative is Vehicle Infrastructure Integration (VII), 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). This initiative builds on recent advances in wireless data communications technologies to establish vehicle-to-vehicle and

---

[3] This initiative began when the Intermodal Surface Transportation Efficiency Act of 1991 created the Intelligent Vehicle-Highway Systems (IVHS) program. As the emphasis shifted from highways to broader advanced transportation technologies, the program was renamed Intelligent Transportation Systems (ITS). More historical details can be found in Glancy (1995, p. 151, at note 3).

vehicle-to-roadside safety applications, what has become known as Vehicle Safety Communication technologies.

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 VII initiative has led to the development of Vehicle Safety Communication (VSC) technologies, intelligent on-board safety applications which 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 from their immediate surroundings, process this information and exchange it with other networked vehicles to provide real-time safety information about the immediate surroundings.

To help facilitate the advancement of VSC technologies, the VII initiative formed a coalition between federal and state transportation agencies, technical standards bodies, and major

vehicle manufacturers. In turn, seven vehicle manufactures formed a cooperative research program called the Vehicle Safety Communications Consortium (VSCC).[4] Four of the main project goals of the VSCC are to (1) identify and evaluate the safety benefits of vehicle safety communication applications, and estimate their deployment feasibility; (2) assess the associated communication and data requirements specific for VSC applications; (3) investigate any issues that might affect the successful deployment of vehicle safety applications; and (4) contribute to the formation of the necessary technical standards and communication protocols (Vehicle Safety Communications Consortium). A summary of preliminary findings has been made publicly available, and are discussed below.

VSC Applications

The VSCC compiled a comprehensive list of over 75 potential safety and non-safety communications-based vehicle applications.[5] After analyzing the anticipated maximum potential safety benefits, and taking into consideration potential market penetration and deployment timeframes, the VSCC focused their attention on eight core applications that were identified with the highest potential safety benefit:

- *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

---

[4] VSC Consortium members are: BMW, DaimlerChrysler, Ford, General Motors, Nissan, Toyota, and Volkswagen.
[5] A complete listing of VSC applications identified can be found in Table 1 in the Appendix of this paper.

- *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

Based on the VSCC analysis, the first three safety applications are categorized as near-term solutions, deployable in the U.S. market between the years 2007 and 2011, while the final five applications have mid-term deployment potential, possibly entering the market between 2012 and 2016. The eight application scenarios selected by the VSCC are viewed as representative of the range of communication and data requirements for vehicle safety applications, and from this group, detailed communication and data requirements have been defined.

Communication and Data Requirements

The safety applications envisioned by VSCC rely on a network of broadcast messages between and among vehicles and roadside infrastructures. This decentralized, point-to-multipoint network will be created utilizing a wireless communication technology called Dedicated Short Range Communication (DSRC).[6] The VSCC considered multiple wireless technologies, including digital cellular, Bluetooth, IEEE 802.11 (Wi-Fi), satellite digital audio radio systems (SDARS), but chose DSRC due to its unique advantages for vehicle safety communication

---

[6] DSRC utilizes a block of spectrum in the 5.850 to 5.925 GHz band allocated by U.S. Federal Communications Commission for the sole purpose of enhancing the safety and the productivity of the transportation system.

applications.[7] Its range of 1000 meters is well suited to the communication of localized information between roadside infrastructure and nearby vehicles, as well as between vehicles in close proximity to one another. DSRC's capability to broadcast messages openly (point-to-multipoint) and in multiple directions is an advantage over typical point-to-point wireless communication technologies, alleviating the need for nodes in the network to be able to specifically identify and establish a communication link with other individual nodes. A final advantage of DSRC is its low latency, the amount of time it takes for a data packet to move across a network connection. The law latency of DSRC allows for the rapid and periodic repetition of short messages consistent with the sensor update and data processing rates envisioned for VSC applications.

The VSCC's analysis of the communication requirements for the eight high-priority vehicle safety applications also helped identify the relevant data message set requirements (Vehicle Safety Communications Consortium, pp. 67-137). Most data messages will likely include location coordinates, time and date, vehicle speed, and a vehicle or message identification number, necessary for the various processing units to keep track of multiple messages received simultaneously. Other data requirements vary depending on the particular application scenario. The Traffic Signal Violation Warning and Curve Speed Warning applications require one-way communication from the infrastructure to the vehicle. For the Traffic Signal application, the message requirements include such data as traffic signal status information, road shape information, and intersection information, including its physical location. The message set data for Curve Speed Warning transmissions include a curve identification code, curve angle, road width, shoulder width and other descriptive data.

---

[7] For comparisons and evaluations, see Vehicle Safety Communications Consortium. *Vehicle Safety Communications Project: Task 3 Final Report: Identify Intelligent Vehicle Safety Applications Enabled by DSRC*, pp. 40-52, and 139.

The Emergency Electronic Brake Lights, Pre-Crash Warning, Cooperative Forward Collision Warning and Lane Change Warning applications require messages to be transmitted from vehicle-to-vehicle. Common data message set requirements among these applications include the vehicle's identification number, GPS coordinates, date and time, vehicle speed, vehicle heading, vehicle size and other data relevant to the vehicles status. The Left Turn Assistant and Stop Sign Movement Assistant applications envision a combination of infrastructure-to-vehicle and vehicle-to-vehicle transmissions, both envisioning message requirements similar to those described above.

Security Considerations

The third responsibility of the VSCC is to identify and investigate key issues that might affect the successful deployment of vehicle safety applications. As of the writing of this paper, *communications security* remains an "open issue" for VSC applications.[8] 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

---

[8] See Vehicle Safety Communications Consortium. *Vehicle Safety Communications Project: Task 3 Final Report: Identify Intelligent Vehicle Safety Applications Enabled by DSRC*, pp. 5, 138.

emergency vehicle). Proposed security solutions include cryptographic mechanisms to ensure the authentication and integrity of messages. Roadside infrastructural units would be issued digital certificates containing authorization information (such as type of unit and geographic location). All messages transmitted from roadside infrastructure would be digitally signed using public key encryption and authenticated by the receiving vehicle. Vehicle-based units would utilize essentially the same encryption protocol as infrastructural units.

Along with the need for authenticity and integrity in VSC data communications, *data anonymity* has emerged as key security issue. Anonymity and privacy are considered key factors in the success of many ITS-related technologies: "If ITS systems are developed and deployed which do not respect the privacy of the American driver, there is a good chance that Americans will demand that the system be shut off. Without strong privacy provisions, ITS will not succeed" (Garfinkel, 1996, p. 324). Since some safety messages may 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). To help facilitate anonymity, one proposal suggests vehicle-based units should be issued multiple digital certificates, making identification or tracking of individual vehicles more difficult. Another proposal suggests using random media access control addresses (MAC addresses) to avoid associating a particular vehicle with a particular MAC address.[9] Various modes of randomization have been suggested: changing at a periodic rate of time, changing

---

[9] A MAC address is an identifier attached to most forms of networking equipment; typically a MAC address is unique to that equipment.

whenever the vehicle falls below a certain speed for a certain amount of time, or assigning a new MAC address each time a vehicle communicates with a roadside unit. At the time of this writing, how anonymity will be built into the design of VSC technology, if at all, remains unresolved.[10]

Standards & Protocols Development

For the automotive companies in the consortium to deploy successfully the eight priority VSC applications, the above security issues must be addressed, and solutions implemented to their satisfaction. To ensure the security needs for vehicle safety applications are met, the VSCC has been active in the development process for communication standards and protocols for the new technology.

The standards and protocol development centers on the 5.9 GHz DSRC wireless technology, and requires coordination between a number of standards bodies: The American Society for Testing and Materials (ASTM), the International Organization for Standardization (ISO), the Society of Automotive Engineers (SAE), the American Association of State Highway & Transportation Officials (AASHTO), the Intelligent Transportation Society of America (ITS), and the Institute of Electrical and Electronics Engineers (IEEE). Each standards body is responsible for a different aspect of implementing DSRC for vehicle safety applications, ranging from the physical architecture of the technology, in-vehicle electronics and interfaces, roadside infrastructure deployment, management of relations with government agencies, and the wireless communications protocols.

The VSCC has been most involved with the IEEE's efforts, participating in its two main DSRC-related working groups: the P1609 working group on Standards for Dedicated Short Range Communications (DSRC); and the P1556 working group on Standard for 5.9 GHz

---

[10] Recommendations for security protocols are scheduled to be made in Spring 2005.

Intelligent Transportation System (ITS) Radio Service Security and Privacy. In particular, the P1556 subcommittee addresses the potential security and privacy threats to DSRC communication, and the means of responding to these threats. This subcommittee consists of a groups of engineers and consultants, including representatives of the VSCC, who meet periodically to recommend and discuss standards for DSRC; at the time of this writing, a final draft standard addressing the potential security and privacy threats is due to be distributed for comments in early 2005.

To summarize, recent advances in wireless data communications technologies have led to the development of Vehicle Safety Communication (VSC) applications. This new breed of Intelligent Transportation System technologies will combine intelligent on-board processing systems with wireless communications for real-time transmission and processing of relevant off-vehicle safety data to provide warnings of hazards, predict dangerous scenarios, and even help avoid collisions. Utilizing ad-hoc wireless networks between multiple vehicles and roadside units, VSC applications broadcast messages about a vehicle's current location, size and speed, or the status of a traffic signal or the recommended rate of speed for navigating a curve. The automotive industry-led Vehicle Safety Communications Consortium has taken a lead role in the development of VSC applications. Particularly important for this paper is the consortium's dedication to addressing the data anonymity issues that might affect the deployment and public acceptance of VSC applications. The VSCC sees data anonymity as a key factor in determining the success of VSC technologies, which has led to an ongoing discussion of whether and how to protect the privacy of a driver's personal information in the design of these systems.

It becomes vital, then, for the designers of these new safety applications to consider how the introduction of VSC technology might disrupt existing values of privacy of personal information in the context of highway travel. How the value of privacy is contextualized is a key factor in designing a technology in a value-sensitive way. The purpose of the next section is to introduce the framework of "contextual integrity" as a means of understanding how the norms of personal data flows might be disrupted by the introduction of new technology.

PRIVACY AS CONTEXTUAL INTEGRITY

Problem of "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 the majority of theorists, 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 non-sensitive (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 non-sensitive (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 trans mit 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. These developments 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 privacy laws and theories, Nissenbaum developed the theory 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. It might be acceptable for me to approach a stranger and offer her a hug at a 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.

The latter examples reveal the ways in which norms govern 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 flow or 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 Flow or Distribution

In addition to appropriateness, the flow or 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 flow prevent my friend from distributing my personal information to a third person. Similarly, norms of flow or 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 of flow 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 flow to govern how personal information is shared within any given context.

Maintaining Contextual Integrity

Contextual integrity 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* impacts the governing norms of appropriateness and flow to see whether and in what ways either of the norms is breached. To 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 VSC 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 VSC applications on the contextual integrity of personal information 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 their names, ages or occupations.

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.[11] 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.

Norms of appropriateness anticipate the sharing of some generally-observable information: non-identifiable 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

---

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

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 Flow 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 flow or 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 actually observe another vehicle. Further, that person would be unable to observe *all* vehicles and would have to 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 flow or distribution.

Other elements of the norms of flow 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 flow 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 of flow on sharing some personal information to third parties.[12] 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 flow 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 flow 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 flow 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 continue to change. One example is the increased use of traffic video 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 flow 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 of flow are 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

---

[12] 103rd Congress, H.R. 3365.

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 flow caused by the introduction of traffic cameras and E-ZPass technologies disrupted the contextual integrity of the flow of personal information in the context 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 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 flow, has not occurred without concern or public debate (see Selingo, 2001; White, 2003).

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. These examples reveal the affects of existing, deployed technologies. When considering vehicle safety communications, the focus of this paper, it becomes crucial to understand that these technological systems are *not yet fully developed*. By predicting the impact VSC might have on the contextual integrity of personal information flows

in the context of highway travel, we can reveal how the design of such technologies implicate the value of privacy while critical design decisions still remain.

VSC TECHNOLOGY AND CONTEXTUAL INTEGRITY

Since VSC technology is still in development, its impact on the flow of personal information has not yet been fully contemplated by privacy theorists or debated in public, let alone challenged in the judicial system. Given the general ambivalence to the problem of privacy in public noted in Section III 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, it is 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 introduction of such a technology might disrupt the contextual integrity of personal information in the context of highway travel. It is vital to understand how the insertion of Vehicle Safety Communication technologies into the context of highway travel might disrupt the existing norms of appropriateness and flow of information. And more importantly, since these VSC applications and standards are still in the developmental stage, the opportunity is ripe to raise awareness and guide the designers to be proactive in support of the existing contextual integrity of the flow 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: non-identifiable 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 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." Similarly, while all vehicles openly display their unique license number, VSC technologies might also transmit a unique identifier. 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. The added precision and accuracy of a transmitted identification number enabled by VSC technology upsets the current norm of only appropriate visual 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.[13] 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 appropriateness.

Potential Impact on Norms of Flow

By overcoming some of the natural barriers to mass surveillance of highway traffic, VSC technologies might also disrupt the norms of flow 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 well-placed 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 technology disrupts the norms of flow further. While traffic cameras allow the archival and retrieval of video surveillance images, the digital nature of the information provided by VSC applications 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

---

[13] 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.

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.

CONCLUSION: INFLUENCING DESIGN TO MAINTAIN 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 personal data flows in ways that threaten the value of privacy. When considering the ramifications of the 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. The standards and protocols that arise from the design process may have significant implications for decades afterwards. VSC designers need to understand how the design and deployment of such technologies might affect the normative standards of personal information flow in the context of highway travel. Yet, as Agre (1994) has noted,

standard-setting processes will presumably "embed a wide variety of political agendas" and the process of developing those standards will be "contested along a variety of fronts by various parties" (p. 84). It becomes vital, then, to engage directly with the VSC design community to raise awareness of the value 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.

The multi-disciplinary perspective known as Value Sensitive Design is well suited to guide this endeavor. Value Sensitive Design has emerged to 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 Friedman, 1999). Recognizing how technologies contain ethical and value biases, the primary goal of Value Sensitive Design is to affect the design of technology to take account for human values during the conception and design process, not merely retrofitted after completion.

By working alongside the researchers and engineers designing and writing the standards for VSC applications, I am in a position, with the help of this paper, to raise awareness of the value implications of their design decisions. Working from within the Value Sensitive Design methodologies, this research will culminate with a set of heuristics to guide the design of VSC technologies. The goal is to enable the development of innovative safety applications that increase traffic safety, but without violating the norms of personal information flow – to maintain the value of "privacy in public."

BIBLIOGRAPHY

Agre, P. (1994). Social choice about privacy: Intelligent vehicle-highway systems in the United States. *Information Technology & People, 7*(4), 63-90.

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

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

Friedman, B. (1999). *Value-sensitive design: A research agenda for information technology* (Contract No.: SBR-9729633). Report to the National Science Foundation [On-line]. Available: http://www.ischool.washington.edu/Value Sensitive Design

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

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.

Selingo, J. (2001, October 25). It's the cars, not the tires, that squeal. *The New York Times*, pp. 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*. Retrieved December 18, 200, from http://www.its.dot.gov/initiatives/initiative9.htm

U.S. Department of Transportation/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* [Brochure]. DOT HS 809 775. Washington, DC: Author.

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.* Washington, D.C.: Electronic Privacy Information Center. Available at http://www.epic.org/privacy/location/jwhitelocationprivacy.pdf.

APPENDIX

Table 1: Communications-Based Vehicle Safety and Non-Safety Applications

(Vehicle Safety Communications Consortium. *Vehicle Safety Communications Project: Task 3 Final Report: Identify Intelligent Vehicle Safety Applications Enabled by DSRC.*)

Safety Applications:

Intersection Collision Avoidance	• Traffic Signal Violation Warning • Stop Sign Violation Warning • Left Turn Assistant • Stop Sign Movement Assistance • Intersection Collision Warning • Blind Merge Warning • Pedestrian Crossing Information at Designated Intersections
Public Safety	• Approaching Emergency Vehicle Warning • Emergency Vehicle Signal Preemption • SOS Services • Post-Crash Warning
Sign Extension	• In-Vehicle Signage • Curve Speed Warning • Low Parking Structure Warning • Wrong Way Driver Warning • Low Bridge Warning • Work Zone Warning • In-Vehicle Amber Alert
Vehicle Diagnostics and Maintenance	• Safety Recall Notice • Just-In-Time Repair Notification
Information from Other Vehicles	• Cooperative Forward Collision Warning • Vehicle-Based Road Condition Warning • Emergency Electronic Brake Lights • Lane Change Warning • Blind Spot Warning • Highway Merge Assistant • Visibility Enhancer • Cooperative Collision Warning • Cooperative Vehicle-Highway Automation System (Platoon) • Cooperative Adaptive Cruise Control • Road Condition Warning • Pre-Crash Sensing • Highway/Rail Collision Warning • Vehicle-To-Vehicle Road Feature Notification

Non-Safety Applications:

Traffic Management	• Intelligent On-Ramp Metering • Intelligent Traffic Flow Control
Tolling	• Free-Flow Tolling
Information from Other Vehicles	• Cooperative Glare Reduction • Instant Messaging • Adaptive Headlamp Aiming • Adaptive Drivetrain Management • Enhanced Route Guidance and Navigation • Point of Interest Notification • Map Downloads and Updates • GPS Correction

Other Potential Applications:

- Green light optimal speed advisory
- Infrastructure-based traffic management
- Traffic information
- Transit vehicle data transfer
- Emergency vehicle video relay
- Border clearance
- On-board safety data transfer
- Vehicle safety inspection
- Driver's daily log
- Access control
- Drive-thru payment
- Parking lot payment
- Data transfer / Info-fueling
- Vehicle computer program updates
- Video downloads
- Vehicle sensing alternative for inductive loop
- Transmitter for bicycle/pedestrian/blind person/etc. (in-vicinity advisory)
- On-call mechanic
- SOS environmental assessment (picture/video)
- Overhead storage reminder (height clearance)
- Drowsy driver advisory
- Distracted driver advisory
- Beacon for child left in vehicle
- Peer voting of driving patterns (commercial vehicle)
- Dynamic emissions tests
- Speed limit assistant
- Parking spot locator
- Electronic license plate
- Electronic driver's license (hazardous waste delivery, etc.)
- Vehicle lock-down (disable a vehicle remotely)
- All-points bulletin (request vehicle with particular identity to respond)