MDOT
Michigan Department of Transportation

CAR
CENTER FOR AUTOMOTIVE RESEARCH

ITS DATA ETHICS
IN THE PUBLIC SECTOR

August 2014

MDOT
Michigan Department of Transportation

CAR
CENTER FOR AUTOMOTIVE RESEARCH

Sponsoring Organization:
Michigan Department of Transportation (MDOT)
425 Ottawa Street
P.O. Box 30050
Lansing, MI 48909

Performing Organization:
Center for Automotive Research (CAR)
3005 Boardwalk, Suite 200
Ann Arbor, MI 48108

ITS Data Ethics in the Public Sector
August 1, 2014
MDOT REQ. NO. 1259, Connected and Automated Industry Coordination
Task A.1. Ethics of Government Use of Data Collected via Intelligent Transportation Systems

Author(s):
Eric Paul Dennis, CAR
Joshua Cregger, CAR
Qiang Hong, Ph.D., CAR
Managing Editor(s):
Richard Wallace, M.S., Director, Transportation Systems Analysis, CAR
Matt Smith, P.E., PTOE, Statewide ITS Program Manager, MDOT
Additional Contributor(s):
Ashley Poindexter, CAR
Yvo Maldonado, CAR
Collin Castle, P.E., MDOT

This report is not to be construed as legal opinion or advice.

Abstract:
This report provides ethical decision-support for transportation professionals involved with *Intelligent Transportation Systems* (ITS) data. Ethical concerns regarding ITS usually focus on travelers' *right to privacy*, and especially *location privacy*. This report establishes core principles of ethical behavior for government use of ITS data using the American lineage of political and ethical philosophy. Furthermore, this report frames foundational ethical beliefs in a contemporary context in order to propose a set of general guidelines for ITS data policies. Finally, this report examines the ethical implications of existing and potential ITS programs managed by the Michigan Department of Transportation.

ACKNOWLEDGEMENTS

This document is a product of the Center for Automotive Research under a State Planning and Research Grant administered by the Michigan Department of Transportation.

EXECUTIVE SUMMARY

The Michigan Department of Transportation (MDOT) is a recognized leader in advanced transportation system technologies, including *intelligent transportation systems* (ITS), and is committed to remaining a source of innovation. The management of cutting-edge projects requires bold leadership and acting without precedent. In keeping with its leadership, MDOT asked the Center for Automotive Research (CAR) to examine several such issues, including ethical issues related to the use of ITS data. In response, CAR conducted new research and built on an earlier (2012) report: *Ethics of Government Use of Data Collected via Intelligent Transportation Systems*.[1] The 2012 report reviewed relevant ethical issues and legal precedent regarding ITS and found, most notably, that existing laws in the United States do not provide clear guidance in the development of ITS programs. Having established in the earlier report that an ethical ITS policy cannot be based on legal precedent alone, in this report MDOT and CAR seek to establish core ethical values on which an ITS data policy can be based.

Ethical concerns regarding ITS usually focus on travelers' *right to privacy* and especially *location privacy*. New ITS tools may include the ability to track vehicles. The potential to track vehicles has recently generated substantial research and discussion about the relationship between ITS and travelers' right to privacy.

To evaluate ITS data policy, public transportation agencies must have an understanding of some complex ethical concepts: What is privacy? What does the right to privacy include? Where did this right come from? And why is privacy *good*, anyway?

The goal of ethical inquiry is to find *first principles*—universal values of what is good and true. This is not easy. Previous research on ITS data ethics has generally embedded the first principle that *people have a right to privacy*, and thus violations of privacy are bad. But this approach is limited because it does not explain what privacy is or why a right to privacy is good. It also does not explain why so many of us are willing to trade our privacy for rather trivial benefits.

[1] An updated summary of the 2012 report is included in the appendices of this report. The original version of the full report can be accessed at: http://www.cargroup.org/?module=Publications&event=View&pubID=91.

This report derives first principles of ethical behavior for government use of ITS data from a Western-American lineage of political and ethical philosophy. We also attempt to show what can be good about surrendering a right to privacy, which individuals often do willingly. Government agencies must often mediate these countervailing values, requiring complex ethical judgments.

This report frames foundational ethical beliefs in a contemporary context and proposes a set of general guidelines for ITS data policy. Furthermore, this report examines the ethical implications of existing and potential ITS programs managed by MDOT. The proposed guidelines are as follows:

1. Recognize any use of personally identifiable information as an ethical decision point.
2. Avoid the creation of personally identifiable information when a practical alternative exists.
3. Recognize the ability to travel anonymously as a socially critical ethical value.
4. Pursue partnerships that allow personally identifiable location data to remain in the private sector.
5. Use informed consent, or opt-in programs, whenever it is necessary to collect personally identifiable location data.
6. Restrict access to personally identifiable information on a need-to-know basis and use best practices in internal data security.
7. Encrypt personally identifiable location data whenever practical and always when transmitted wirelessly or over public networks.
8. Do not rely on data scrubbing alone to protect personally identifiable information.
9. Use data aggregation techniques whenever possible to minimize use and distribution of personally identifiable information.
10. Destroy raw data files containing personally identifiable information as soon as practical.
11. Share personally identifiable information only with third parties that can be trusted to use the data as originally intended.
12. Recognize that any data has the potential to be used for law-enforcement, even if this is not the original intent.

TABLE OF CONTENTS

MDOT
Michigan Department of Transportation

CAR
CENTER FOR AUTOMOTIVE RESEARCH

1 INTRODUCTION

This report is about ethics. Specifically, it is intended to provide ethical decision-support to transportation professionals working in the field of *intelligent transportation systems* (ITS), with special attention to the use of the data generated by such systems.

Our understanding of technology usually lags behind its capabilities. Today, transportation agencies can utilize advanced ITS technologies to improve the safety, mobility, and efficiency of the entire transportation system. The astonishing potential for what *could* be done obligates us to consider what *should* be done. The ethical implications of advanced ITS have prompted the Michigan Department of Transportation (MDOT) and Center for Automotive Research (CAR) to investigate the issues.

To illustrate why MDOT is seeking ethical guidance for ITS data policy, consider a hypothetical department of transportation (DOT) manager thinking about investing in a new ITS deployment: The engineers tell her it will provide reliable data, the lawyers assure her that it is legal, and the accountants calculate that it will save money. The manager remains undecided. This hypothetical ITS tool records not only the speed of traffic, but also the *bodyweight* of drivers and passengers. Even though the engineers, lawyers, and accountants say it is the correct decision, she does not know if it is the *right* thing to do.

After considering the benefits and costs of the new ITS tool, our hypothetical agency manager decides against it. She decided that recording peoples' bodyweight would be a violation of their privacy. Although she could not imagine any way that the data could be traced back to individuals or used against them, it just, somehow, seemed *wrong*.

People are often faced with decisions like this (especially in middle management). If the preferred course of action were obvious, it would not be a decision; it would have been done already. In the hypothetical above, our DOT manager balanced the value of cost-savings against the loss of privacy and decided it was not worth the trade-off.

How was she able to measure the value of privacy? Possibly, she went with 'gut-feeling;' She felt that she would not want her bodyweight recorded and was inclined against it as a public policy. But the personal preference of government employees is not an appropriate basis for public policy. Ideally, she tried to put aside her own values to consider her role as a professional agent of the DOT.

Even then, how should *an agency* make ethical decisions? In formal practice, government accountants attempt to monetize ethical values, providing such strange facts as a ‘statistical life’ being worth $9.2 million. This does not help much in the routine business of running an agency. In day-to-day matters, complex ethical choices often get decided by gut-feeling, or moral intuition.

Human intuition is a useful tool in ethics and otherwise. The trained intuition of experienced professionals can be a very useful tool. Nobody should completely ignore their gut. But our world is complicated. Intuition can be wrong. Our guts can be fooled. Moreover, our guts probably are not prepared for the task of intuiting as an ethical proxy for a modern state government.

While it is understandable for individuals to bring their personal values into ethical decisions, ideally these decisions will also consider the values and ethics of the agency and government being represented. This report is intended to provide public agencies with ethical decision-support for situations where law and policy do not provide clear guidance. Specifically for ITS data use, this report explains why people value privacy and how transportation agencies should incorporate such values in the design, deployment, and management of ITS programs.

2 ETHICAL CONSIDERATIONS OF GOVERNMENT AGENCIES IN DATA POLICY

The study of ethics is the study of values. What makes a thing good or bad? What makes an action right or wrong? Casual ethical decisions usually call on our *morality*—our personal sense of right and wrong. Morality will naturally factor into ethical discussions. However, the potential for moral disagreement between individual people requires that agencies seek to establish common ethical principles. This chapter introduces a framework to help guide public policy discussions regarding data ethics.

2.1 LEGAL GUIDANCE

Considerations of data policy should first seek guidance from applicable laws, regulations, and legal precedent.[1] Unfortunately, existing laws provide almost no guidance for data use in ITS programs.[2] Legislatures and courts have had very little to say about transportation agencies' responsibilities regarding ITS.[3]

There is some case law regarding technologies relevant to ITS data, such as Global Positioning System (GPS) tracking.[4] But essentially all legal precedent focuses on how such technologies are used in law-enforcement. It is unclear how such precedent would apply to ITS deployed for system administration.[5]

Trying to extrapolate existing case law to potential ITS-related jurisprudence would likely provide more confusion than clarity. Moreover, legal analysis is not sufficient to develop ethical guidelines. Ethics are not derived from laws. In fact, the opposite is true.

Laws can be thought of as the formalization of normative ethical principles. Ethical foundations may be excavated from legislative text and interpretations,

[1] Professional societies such as the National Society of Professional Engineers (NSPE) and the American Institute of Certified Planners (AICP) also have formal codes of ethics. While these codes provide guidance regarding neglect and malfeasance, they are not generally specific enough to provide decision-support to ITS data policy decisions.

[2] Douma and Aue 2011.

[3] Hong, Cregger, and Wallace 2012.

[4] Hong, Cregger, and Wallace 2012.

[5] A recent case, *U.S. v. Jones* (2012), is occasionally referenced in the context of ITS as it involved government GPS tracking of a vehicle. However, the majority opinion centered on ideas of trespass (i.e., the physical planting of a GPS tracker on a private car as part of a police action). This is not relevant to ITS. If anything can be learned from this case relevant to ITS, it is probably in Justice Sotomayor's concurring opinion.

but this is a convoluted and error-prone method of constructing ethical guidelines for new contexts such as ITS. Learning about the ethics of a society by examining its laws would be like learning about the fish of the ocean by examining the contents of a shark's stomach (Figure 1).

The text of a law is meaningless without the ideas beneath it. Finding ethical guidelines for the use of ITS data requires examining foundational ideals of our legal and social systems. When one traces the ideas that inform our ethical intuition and discussions of data use, it appears that formal legal precedent plays a relatively minor role. More controlling are cultural beliefs that we have inherited from the Western tradition of ethical philosophy.

Figure 2 represents the primary ideological influences and their relationship to ITS data ethics as determined by CAR analysts' research and analysis. Figure 2 should not be interpreted as a definitive or formal reduction of ITS data ethics. It is provided as one possible model regarding how complex ethical ideas have evolved over the preceding millennia.

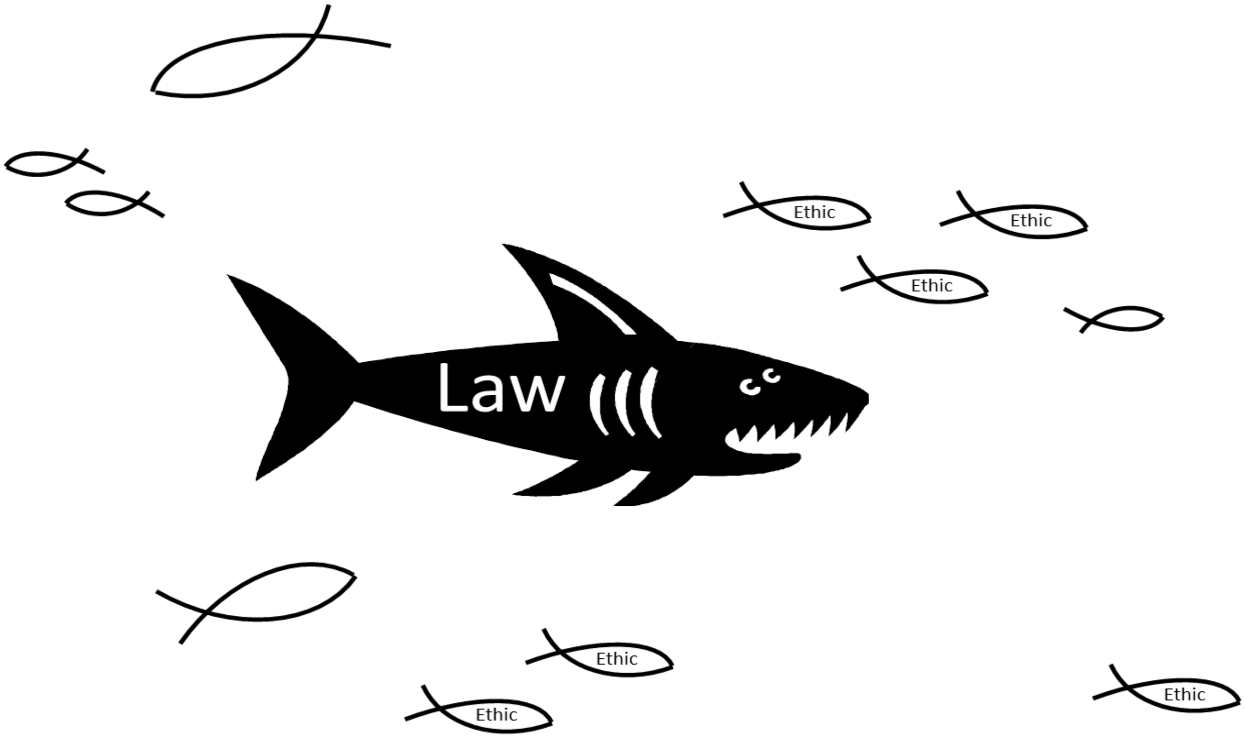

FIGURE 1: ETHICS IS TO LAW AS FISH ARE TO A SHARK'S STOMACH

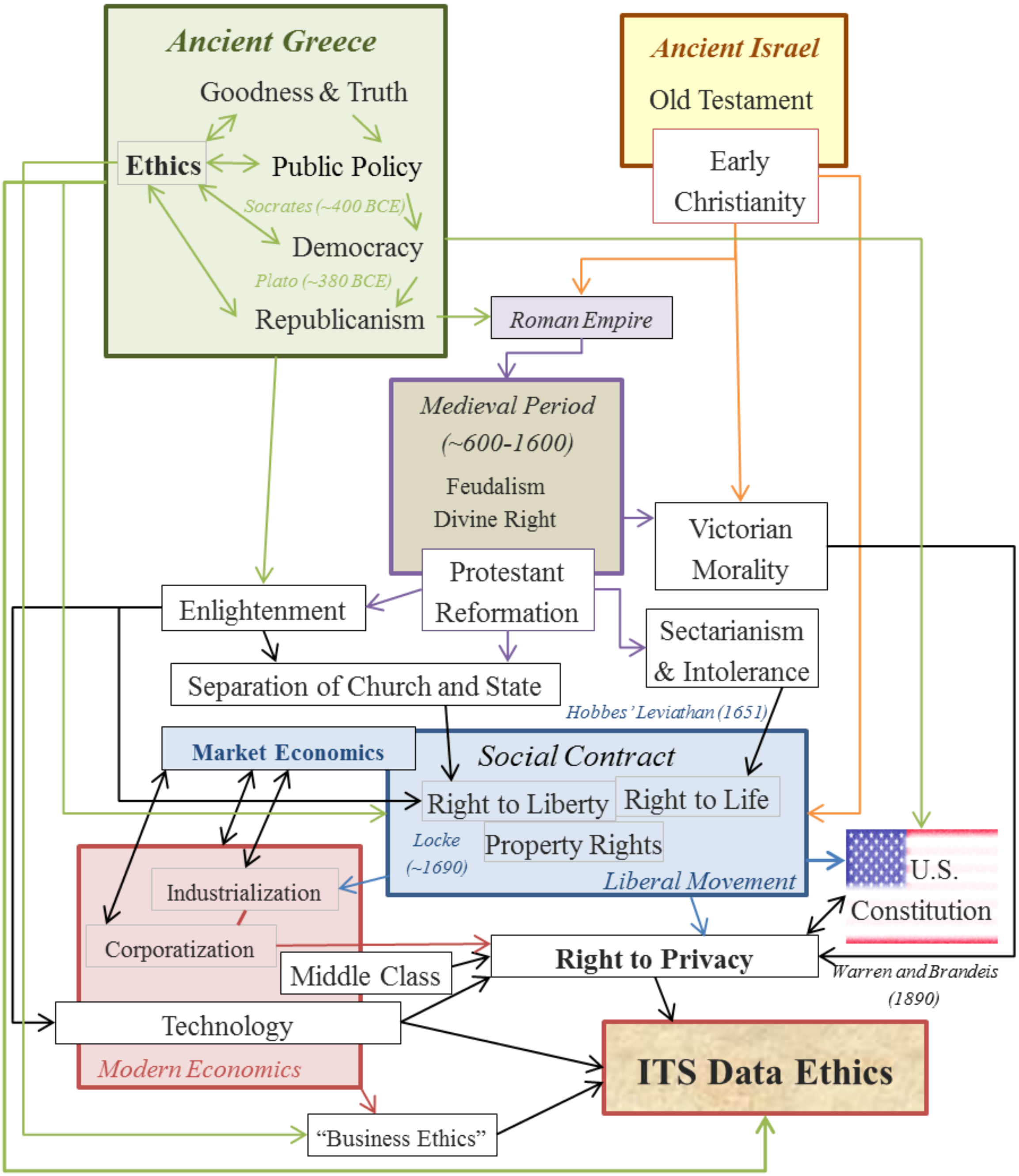

FIGURE 2: SOURCES OF IDEAS INFORMING ITS DATA ETHICS

2.2 ETHICAL JUSTIFICATION FOR PUBLIC ADMINISTRATION

In the United States and most developed countries, it is taken for granted that we should generally respect the laws created and enforced by government. It seems obvious that there should be laws. Though we may occasionally ignore some laws (e.g., jaywalking, speed limits, etc.) we find living in a law-governed society to be as natural as breathing air. But in the scope of human experience this situation is rather unusual.

The United States is among an elite group of nations that has a *powerful central government*, a *strong rule of law*, and *democratic accountability*. The stable balance of these three components has been identified as prerequisite to a successful modern *liberal democracy*[6] by political scientist Francis Fukuyama, who notes, "The fact that there are countries capable of achieving this balance constitutes the miracle of modern politics."[7] Fukuyama goes on to describe that maintaining this balance requires a dynamic tension of opposing interests:

> The state ... concentrates and uses power to bring about compliance with its laws on the part of its citizens. ... The rule of law and accountable government, on the other hand, limit the state's power, first by forcing it to use its power according to certain public and transparent rules, and then by assuring it is subordinate to the will of the people.[8]

The theories by which a central government holds legitimate authority are complex and eternally under debate. Even today, there is broad disagreement over what should be considered ethical government action. It is evident, however, that sustainable government institutions must balance the needs of the state with the civil liberties and rights of its people.[9]

[6] The word *liberal* in this report is not used in the contemporary American political way. *Classical liberalism* can generally be interpreted as a separation of state functions from religions institutions and market economics.

[7] Fukuyama 2011, 16.

[8] Fukuyama 2011, 16.

[9] The most primary need of a state (i.e., a commonwealth or nation) is to remain a state. This understanding leads to recognizing the foundational state functions as *taxation* (in order to finance state activities), *conscription* (raising of armies for national defense), and *prevention of rebellion*. Such functions necessarily restrict autonomy of citizens. For more, see Scott 1998.

THE ROOTS OF GOVERNMENT ETHICS

An ethical government agency can be expected to first seek guidance in existing law, regulation, and policy. When such a search fails to provide guidance, it may not be immediately clear how to proceed.

Decision-makers in public agencies may assume that the ethical reasoning of long-dead philosophers would be completely irrelevant in this day and age. This would be wrong. In truth, nearly everything that we say, do, and think has been influenced by some long-dead philosopher.[10] Many ethical principles that we thoughtlessly accept today can be traced back about 2,500 years to a few Greek city-states.[11] The aura of ancient Greece seems invisible to us now, only because it is all around us.

The teachings of Socrates (around 400 BCE) are often understood as a paradigm shift in government ethics. Socrates was continually occupied with the problem of getting competent, ethical men into positions of power. He understood statecraft as the art of acting in the public interest and requiring particular knowledge and training.

> He would ask such questions as: ‘If I wanted a shoe mended, whom should I employ?’ To which [the student] would answer: ‘A shoemaker, O Socrates.’ He would go on to carpenters, coppersmiths, etc., and finally ask ... ‘who should mend the Ship of State?’[12]

Socrates was tried, convicted, and executed by citizen jurists on the charge of ‘corrupting youth.’ While records of the trial are incomplete, it seems that Socrates’ most corrupting influence was teaching that it is proper and good to question authority. Such controversial ideals of government accountability have become self-evident to us today.

Plato, a student of Socrates, inherited Socrates’ preoccupation with the ethical principles of governance and what makes a good society. Plato’s *Republic*

[10] As John Maynard Keynes said: “Practical men who believe themselves to be quite exempt from any intellectual influence, are usually the slaves of some defunct economist. Madmen in authority, who hear voices in the air, are distilling their frenzy from some academic scribbler of a few years back.”

[11] Russell 1946. This should not be interpreted as suggesting that the ancient Greeks invented morality or ethics. They inherited a moral history and tradition, as we have from them. But the Western tradition of the formal study of ethics hits a dead end in ancient Greece, due mostly to the lack of records previous to this time.

[12] Xenophon, a student of Socrates, quoted in Russell 1946.

describes a communist utopia governed by an elite class of philosophers who would be trained in recognizing public good and acting to achieve it. While the details of *Republic* seem strange to a modern reader, it has had a lasting influence on the role of government in society. Many of the ethical principles described by Plato influence the moral and ethical values of modern Western culture to this day.[13] Westerners inherited from Plato a sense that governing a state requires acting in the public interest, often against the wishes of a public majority.[14] The tension between democratic Athens and Plato's *Republic* reflects a perpetual theme in political philosophy: how best to distribute sovereign power.

Common Era Western civilization retained tendencies towards centralized government power. The adoption of Christianity in Western nations was often leveraged to justify state authority. For the 1,000 years or so known as the Medieval Period,[15] ethical inquiry was bounded by Church doctrine and authoritarian fiefdoms. During this time, rulers often invoked the idea of *divine right*—that kings were endowed by God with unlimited authority and should be unquestioningly obeyed.

It was not until the Protestant Reformation of the sixteenth century that political philosophers gained some freedom to explore the ethical basis of state sovereignty apart from divine right. The Reformation had weakened the power of the Church such that religious leaders were unable to gain control of government. But Protestant leaders were unwilling to submit fully to a king as they were to a pope. This stalemate of opposing forces provided a separation of church and state powers that had been absent from the Western world for centuries.[16] After the Reformation, finding a philosophical justification for government power and public administration suddenly became imperative.

[13] Russell 1946.

[14] Such a majority, for example, may wish to unjustly persecute a minority group within the state. Plato may have been influenced by the success of non-democratic Sparta, and the fact that his friend Socrates had been executed by a citizen jury.

[15] Also called the Middle Ages, roughly considered 600 to 1600 A.D.

[16] Russell 1946.

THE SOCIAL CONTRACT

> "ALL MEN EQUALLY, ARE BY NATURE FREE."
> ~HOBBES (1651)

Much of the basis for modern government ethics is described by Thomas Hobbes in *Leviathan* (1651). Hobbes rejected the divine right of kings and wrote that all men are created equal in rights; every man desires to secure his own life and liberty and has the *natural right* to do so. Hobbes also believed, however, that human nature is such that we are compelled to violate the rights of others by a primal impulse for self-preservation.[17]

Hobbes argued that to avoid an eternal cycle of violence, men seek to balance liberty and security by means of a societal covenant, or *social contract*. The social contract grants a *sovereign authority* (i.e., a central government) the power to make and enforce laws. Those under contract are protected from certain violations of their own liberties by agreeing to give up certain rights to the state. So, for example, a citizen of a sovereign state gains the right not to be murdered in exchange for his or her right to murder others.

This trade-off of rights in the social contract provides an ethical justification for government action without reference to divine right. A sovereign state is endowed with a monopolistic right to physical violence in order to enforce the conditions of the social contract. Citizens of a state agree to be subject to police power in order to secure the freedoms gained by living under a rule of law. Without the threat of force, the contract would be ineffective.[18]

The liberal movement that followed Hobbes adopted his idea of social contract, but felt that the sovereign power would tend towards tyranny unless limited with multiple checks and balances on sovereign power.[19] John Locke was one of the most influential of the liberals, writing two *Treatises on Government* in 1689 and 1690. The *First Treatise* criticizes the theory of

[17] Hobbes famously described the life of man in the *state of nature* as "solitary, poor, nasty, brutish, and short." The idea of a state of nature—how man behaves outside of government—became central to the theories of Hobbes, Locke, and many political philosophers of the era.

[18] Hobbes writes, "Covenants, without the sword, are just words."

[19] Hobbes envisioned a monarchy to be the best type of government to weld sovereign power effectively enough to maintain law and order. He accepted the possibility of absolute power leading to corruption, but thought it was unlikely. He believed that if citizens strictly maintained the contract, the monarchy would remain benevolent. While Hobbes preferred monarchy, his abstract argument is applicable to all forms of government, including democracy.

sovereignty as justified by divine right and heredity. In the *Second Treatise on Government*, Locke sought to establish a more defensible basis for political power.

Locke's *Second Treatise* borrows much from Hobbes, but in contrast to Hobbes (who imagined life without government as "nasty, brutish, and short"), Locke viewed humans as naturally capable of peaceful self-governance according to *reason*.[20] As recounted by Bertrand Russell, Locke imagines that without government, humans would live as,

> ... virtuous anarchists, who need no police or law-courts because they always obey 'reason', which is the same as 'natural law,' which, in turn, consists of those laws of conduct that are held to have a divine origin. (For example, 'Thou shalt not kill' is part of natural law, but the rule of the roads is not.)[21]

Locke, like Hobbes, believed that men were endowed with natural rights and called on the social contract to protect those rights. But in contrast to Hobbes, Locke maintained that the sovereign power was also bound by certain responsibilities to the social contract. When a government oversteps its natural authority, citizens have a right to revolt. Both Hobbes and Locke derived their concept of natural law from Judeo-Christian scripture.[22]

A crucial aspect of Locke's justification for government is the institution and protection of property rights. According to Locke, "The great and chief end of men uniting into commonwealths, and putting themselves under government, is the preservation of their property."[23] The protection and security of property rights was viewed by the liberals as essential for economic growth and national prosperity. The emphasis of property rights in the foundational philosophy of modern Western government has had a significant influence on the later concepts of privacy rights as an essential civil liberty.

Locke was explicit that government power should be limited to the protection of individual rights and private property. Further, government power should

[20] Generally, Hobbes emphasizes the right to life and fears anarchy (state of war) above all. Locke emphasizes the right to liberty and fears tyranny (state of oppression) above all.
[21] Russell 1946.
[22] Russell 1946; Hobbes 1651; Locke 1690.
[23] Locke 1690.

be diffuse and accountable to the people.[24] The development of government organization and ethics in the United States can be traced back through the U.S. Constitution and Declaration of Independence directly to Locke and the liberal movement. Contemporary political arguments regarding subjects such as civil liberties, property rights, and government-overreach stem directly from the ideals formed in the liberal movement, even if the people participating in such arguments are unaware of this influence.

THE UNITED STATES CONSTITUTION

In the United States, the distribution of government power is built on a framework provided by the U.S. Constitution. But it was not a foregone conclusion that this framework would allow for the stable balance of power, rule-of-law, and accountability that Americans enjoy today. Contemporary government agencies operate within the context of a long and complex history marked with frequent violence and disorderly periods. A modern democracy is a complex system with inscrutable inner workings, relationships, and interdependencies. The sociopolitical machinery that now allows the United States to operate as a modern liberal democracy developed incrementally over the preceding millennia.

We should not allow the recent era of relative peace to lull us into believing that our political system is resilient against large shocks. A sudden shift in power structures could cascade across organizations and institutions and threaten the stability of the nation.

The Constitution, alone, is not sufficient to ensure that the current state of institutional stability and domestic peace will continue. In modern liberal democracies, the social contract implicitly establishes the power relationship between a government and its people. Government creation and use of data can significantly alter this power relationship and thus quietly change the terms of the social contract.[25] The world is very different from when the U.S. Constitution was authored in 1787. In today’s world of electronic surveillance, digital records, and data analysis, government agencies and policymakers should consider that possible unintended consequences of data use could

[24] Locke’s vision of government accountability was generally democratic. However, he assumed that only property-owning men (explicitly not women) would have full rights of citizenship.

[25] http://www.forbes.com/sites/bradpeters/2012/07/12/the-age-of-big-data/, accessed February 2014.

cause a big upset in the balance of state power, rule of law, and accountable government.

2.3 GOOD GOVERNANCE AND DATA POLICY IN CONTEMPORARY SOCIETY

It is through public administration that a state is able to exercise power. A sustainable government must be capable of effective and efficient public administration. In order to effectively administer government programs, government agencies are tasked with transforming society into a comprehensible abstraction; this requires data. This essential function of public administration turned early modern governments into archetypical data analysts.[26]

Government data in the digital age has unique implications. Knowledge truly is power. Information can be an instrument of violence if used by a state to control or coerce citizens. Information technology has advanced far beyond that famously imagined in George Orwell's *Nineteen Eighty-Four*—a dystopian novel depicting life under the constant surveillance of an authoritarian state. The digital profile that we create in the course of our daily lives is sufficient that a motivated *adversary*[27] could know much about us without the hassle of personal surveillance.[28] Most of us do not perceive the information age as a surveillance state, but clever data-mining may unearth our private selves to an extent that Orwell could not have imagined. The capabilities of surveillance by data-mining have become so effective that some privacy experts have created a new term to describe it: "überveillance."[29]

Politicians, policymakers, and courts have historically responded to advancements in data technology by codifying privacy rights in law. However, information technology and data science are advancing more rapidly than ever. The legal and ethical frameworks that have formed in the wake of the computer revolution fall short of providing sufficient guidelines for government agencies to enact appropriate data policies. Public agencies

[26] Scott 1998.

[27] The word *adversary* is used in computer science literature to refer to someone who is using data in ways for which it was not originally intended.

[28] Iqbal 2009, 51 describes this as "dataveillance."

[29] Iqbal 2009, 52.

must now determine how to utilize the latest technologies without clear legal precedent or ethical guidance.

POLICE POWERS AND CIVIL LIBERTIES

A state and its government agencies operate with *sovereign authority*. In other words, a state is only subject to those laws by which it agrees to abide. A sovereign state is endowed with certain *police powers* to enforce law and order within its territory. Police powers do not specifically refer to the right of a government to create police forces (though they include this right). The term applies to any measures taken to protect the *safety, health, welfare, and morals* of the community.[30] The police powers of a sovereign state provide the theoretical justification for the state to take actions that may otherwise be opposed by citizens. (For example, this would include the deployment of vehicle-tracking ITS for system administration.)

Civil liberties are the rights of persons within the state that are recognized by the state. These rights often limit the ability of the government to use police powers. Some civil liberties are formally recognized in the U.S. Constitution or those of the states. For example, the First Amendment to the U.S. Constitution says:

> Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble...

Thus the U.S. Constitution explicitly recognizes individuals' rights to religion, speech, and peaceable assembly. However, even these enumerated rights are not absolute. Governments regularly use police power to limit the ability of persons to exercise religion, speak freely, and peaceably assemble. Often

[30] Such language is included in the Tenth Amendment to the U.S. Constitution. http://legal-dictionary.thefreedictionary.com/Police+Power, accessed January 2014. Some may find it strange to conceive of police power as protecting morality, but considering an appropriately broad definition of morality (and ethics), it is probably unavoidable. Government laws, programs, and institutions lend structure to a society and necessarily influence the ways of living that a society comes to see as normal. Even without overt government actions that address moral issues, public policy (or lack-there-of) can quietly influence the normative ethics and morality of people on a generational timescale. Plato's *Republic* discusses such ideas at length, and in fact prescribes rather strict censorship.

these rights are infringed upon for very good reasons, such as limiting one's freedom (of speech) to falsely yell ***fire*** in a crowded theatre.[31]

Justified exercises of police power must balance the interests of the state against the rights of individuals (Figure 3). Some political theorists are concerned that modern liberal governments overemphasize the use of police powers to improve the welfare of a community. While the state's actions may be motivated by the public interest, excessive intervention could quietly erode essential civil liberties. [32] Economist Friedrich Hayek famously described this in *The Road to Serfdom* (1944).

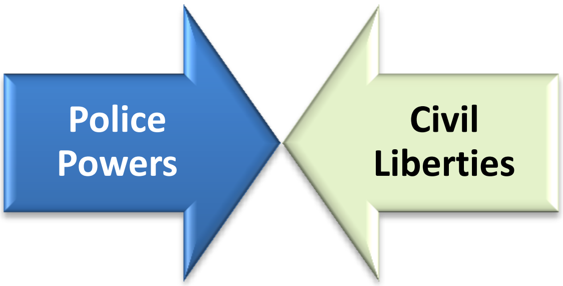

FIGURE 3: A SOVEREIGN STATE MUST BALANCE POLICE POWERS AND CIVIL LIBERTIES (THE DEPLOYMENT OF PUBLIC ITS IS A POLICE POWER)

Drawing from John Locke and the liberal tradition, the American political system is designed to peaceably prevent a slide into tyranny by institutionalizing a series of checks and balances by which various parts of the government can stop other parts of the government from abusing power. While robust, this system of checks, balances, and bureaucracy depends on the moral determination and ethical proficiency of government officials and employees. A functional democracy requires that government agents, from lawmakers to civil servants, must individually and collectively use state authority within boundaries that consider the balance between state interests and civil liberties. Considering government creation and use of data, it is essential to consider that data may not always be used as originally intended.

[31] *Schenck v. United States* (1919). The case was not literally about a fire in a theatre, but was used as an analogy by Justice Oliver Wendell Holmes: "The most stringent protection of free speech would not protect a man in falsely shouting fire in a theatre and causing a panic."

[32] Malloy 1991.

LESSON FROM HISTORY: WORLD WAR II INTERNMENT OF JAPANESE AMERICANS

The U.S. Census Bureau has a constitutional duty to conduct a decennial census to balance citizen representation in the U.S. Congress. Since its creation, the scope of the Census Bureau has expanded greatly to include an array of social and economic statistics. Census data is extremely valuable for public administration and research. However, the use of Census data contributed to what is now considered a regrettable abuse of police power by the federal government:

Following the Japanese attack on Pearl Harbor during World War II, the United States interned over 100,000 people of Japanese descent in "war relocation camps."[33] The internment program took both foreign nationals and American citizens. The newly institutionalized War Relocation Authority[34] was able to target neighborhoods known to house people of Japanese descent as shown by Census data.[35] Furthermore, in at least one instance, a Census Bureau official provided raw survey data, including the names and addresses of families reporting Japanese ethnicity.[36]

While the Census data was originally collected for administrative purposes, it was used by law enforcement to detain suspected enemies of the state. The lesson is that as state agencies consider the ethics of data creation and use, decision-makers should be aware that once data is created, it has the potential to be used in ways that the agency did not intend and may not consider ethical.

BIG DATA AND THE CLOUD

Recent advancements in data science and various technologies are providing new opportunities to public agencies, as well as imposing new challenges. Government officials and agency administrators can be justifiably confused about how to appropriately utilize the latest information and communications technologies. In just the last few years, there has been an increasing sense of a

[33] Individuals of German and Italian descent were also interned, though to a much lesser extent.

[34] The War Relocation Authority (WRA) was a temporary federal police agency specifically created by President Roosevelt to administer the internment effort.

[35] Ohm 2011, 1757.

[36] Minkel, J.R. *Confirmed: The U.S. Census Bureau Gave Up Names of Japanese-American in WW II*. Scientific American. March 30, 2007. Accessed January 2014 at: www.scientificamerican.com/article/confirmed-the-us-census-b/Min

fundamental shift in how government agencies, as well as private organizations, should approach data use and management.

Many advancements have been grouped together and given abstract terms, such as ‘big data’ and ‘the cloud.’ The technologies and institutions underlying these concepts are complex. Comprehensive and definitive review of them is outside of the scope of this report. However, it is worth outlining generally what is meant by these terms and how they may affect the ethics of public administration.

In general terms, the word *data* refers to a set of facts or observations that provide information. Twentieth-century digital technologies led to the development of computer database applications, allowing us to manipulate and understand data in ways never before possible. *Big data* simply refers to advanced technologies and methods that allow even better manipulation and understanding of data over what was possible with twentieth-century databases.

Big data has been made possible in part by the expansion of digital technologies into various aspects of our lives. When we use such technology, we often create data about ourselves.[37] Various software programs record our activities as we interact with digital devices. These records may be saved to archival record files, or *log files*.

New methods and technologies allow data scientists to make this initially disconnected and unstandardized data comprehensible and usable. New capabilities in data-mining could allow a savvy adversary to use publicly available digital information to reconstruct various facts about a user, many of which may be thought private.

Organizations that we trust to secure our personal data (e.g., banks, insurance agencies, email providers, etc.) often provide such data to third-parties on the assumption that it has been ‘scrubbed’ of personally identifiable information. This new age of big data, however, implies that it is essentially impossible to reliably anonymize data by removing identifying elements alone.[38] Without

[37] Even simple smartphone-based games often collect a surprising amount of personal information. http://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data, accessed February 2014.

[38] Ohm 2010. Ohm recommends ending use of the term ‘anonymization’ to describe this process because he believes it inaccurately suggests that such data cannot be reidentified.

breaking any laws, an adversary could potentially reconstruct/reidentify enough about a user to stalk, blackmail, or otherwise cause harm.[39]

The use of big data by government agencies will be the subject of political arguments and policy discussions for years to come. The amount of information available to a government about its citizens is unprecedented. This has potentially significant effects on the power dynamics between a government and its constituents.[40]

A compounding issue is the potential for adversaries to illicitly obtain personal data by 'hacking' into protected servers or devices. The potential for unauthorized access of data may be compounded by *the cloud*.

The cloud is basically just *the internet*—the worldwide network of networks and computers linkable though Internet Protocol (IP) addresses.[41] However, the cloud metaphor does reflect recent changes in the nature of the internet. Until recently, moving data between computers and between networks was relatively slow. Limitations on digital communication technology implicitly restricted remote access to large amounts of data. It was practically necessary to have direct physical access. In other words, working with a database basically required that the database and its software be stored on the users' network. This is no longer the case.

New IT technologies have allowed for the transmission of digital information at speeds sufficient to access and manipulate large amounts of data remotely. The data is not literally floating overhead in a cloud; it still must reside on electronic hardware somewhere in the physical world. However, it is no longer particularly important where that might be, and it is often difficult even to know.

Cloud storage and computing—the use of remote machines for data storage and processing—can be a useful IT strategy for large organizations such as government agencies. Cloud services could provide agencies with high quality low cost IT and data services. A potential drawback is that data hosted on

[39] Obviously these secondary activities would be against the law. The point is that accessing the data that would allow for these activities may not be.

[40] http://www.forbes.com/sites/bradpeters/2012/07/12/the-age-of-big-data/, accessed February 2014.

[41] Cloud computing (in the form of email) actually predated the institution of the TCP/IP stack, and thus is older than the World Wide Web—what we now consider the internet.

remote machines could be vulnerable to unauthorized access. Data owners must generally trust the cloud service provider to secure and protect user data.

In the early decades of database technology, most organizations hosted database servers internally. In many cases, the servers were not connected to the internet, making unauthorized access very difficult. Even when internet connectivity became ubiquitous, external access was inherently limited by slow data transmission speeds in addition to any encryption, firewalls, or other security measures adopted by system administrators. In today's world of high speed internet, once an adversary gains access to data files, they can quickly manipulate or steal large amounts of data. This risk is not specific to cloud-hosted data. Any device connected to the internet is vulnerable to attack.

As state agencies update their IT and data policies, it is important to be aware of the latest and best practices in cyber security. The claim that personal data can be protected by de-identifying or 'scrubbing' it is no longer supportable. Data security technologies can provide a good deal of protection, but cannot guarantee protection from motivated adversaries. Any data can become vulnerable to unauthorized access and unintended use.

U.S. NATIONAL SECURITY AGENCY LEAK OF 2013

A great deal of security can be achieved by storing data on servers or devices that are not connected externally (e.g., to the internet). Many sensitive datasets are stored and used within such secure networks. This physical separation between the internet and a network essentially prohibits remote access. But data leaks still occur.

Many data leaks are accidental, such as an agency employee having a laptop stolen or losing a storage disk.[42]

Some leaks are intentional. In 2013, Edward Snowden, an employee of a contractor to the National Security Agency (NSA) of the United States, leaked massive amounts of classified data to press agents at *The Guardian* and *The Washington Post*. Snowden was able to access the data as a system administrator for an NSA facility. While working for the NSA, he secretly copied hundreds of thousands of files from the secure NSA facility network. The most immediate lesson from the Snowden leak is that threats to data

[42] http://www.computerworld.com/s/article/9234098/Lawsuit_possible_in_NASA_laptop_theft , accessed January 2014.

security can come from inside. Agencies should take care to limit access to sensitive data and institute internal accountability rules.

More importantly, the leaked NSA files and subsequent discussions have profound implications for state agencies concerned with ethical data use in relation to the social contract and checks on government power.[43] A key revelation is that the NSA interpreted a provision of the Patriot Act to perform bulk surveillance that could potentially collect data on anyone.

While supporters of the surveillance program maintain its legality, there does seem to be agreement that something isn't right. The federal government has taken action to reform the program such that bulk data is still collected, but the NSA has reduced ability to access it.[44] Additionally, the Senate has introduced legislation that would reinforce the program with clear legal authority—a tacit acknowledgement of the uncertain legal status of dragnet surveillance.[45]

Many critics of the NSA surveillance program question the legality and constitutionality of bulk surveillance, and recommend ending the program. One U.S. senator has complained that constitutionally mandated oversight of the NSA has been "stonewalled" by a "culture of misinformation," and that the ability of U.S. citizens to trust federal government intelligence agencies,

> ... has been seriously undermined by senior [NSA] officials' reckless reliance on secret interpretations of the law, and battered by years of misleading and deceptive statements that senior officials made [that] hid bad policy choices and violations of the liberties of the American people.[46]

Intelligence agencies, by their nature, are trusted with powerful data. The misuse of such power is dangerous to the principles of checked power and

[43] For example, http://www.intelligencesquaredus.org/images/debates/past/transcripts/021214%20Snowden.pdf, accessed February 2014.

[44] http://arstechnica.com/tech-policy/2014/01/obama-lays-down-new-limits-on-nsa-with-more-reforms-to-come/, accessed February 2014. Reforms include requiring private-sector companies to keep archival data so that it may be subpoenaed by the NSA if needed.

[45] https://www.aclu.org/blog/national-security/dianne-feinsteins-fake-surveillance-reform-bill, accessed February 2014.

[46] Senate Select Committee on Intelligence, January 29 2014. http://www.intelligence.senate.gov/hearings.cfm?hearingid=138603a26950ad873303535a630ec9c9&witnessId=138603a26950ad873303535a630ec9c9-0-1, accessed February 2014.

government accountability. Efforts to provide formal oversight of intelligence agencies must remain a critical focus of policymakers. However, it is notable that data cannot be misused if it cannot be obtained, and cannot be obtained if never created. As state agencies address ethical considerations of how data is created, used, and managed, it is relevant to address the risks of such data being available to intelligence and law-enforcement agencies that tend to periodically test the limits of their power.

2.4 GOVERNANCE CULTURE IN THE STATE OF MICHIGAN

The United States system of *federalism* distributes sovereign authority and police powers between a national federal government and each individual state. This dynamic has resulted in state governments developing unique structures, practices, and cultures. What is considered an appropriate data policy in some states may not work in Michigan.

A state's cultural and political histories shape its public institutions, and are in turn reflected in the values and culture of those institutions. According to data ethicist Kord Davis,

> In many ways, an organization's business processes, technical infrastructure configuration, and data-handling procedures can be interpreted as a manifestation of their values. A responsible organization ... is concerned both with handling data in a way that aligns with its values and with being perceived by others to handle data in such a manner.[47]

In other words, core ethical principles of an agency can often be found in the existing policies and practice of an agency, even when the underlying values are never stated explicitly.

MDOT MISSION

An organization's ethical core is often expressed formally in a *mission or vision statement*. MDOT's stated mission is to:

> Provide the highest quality integrated transportation services for economic benefit and improved quality of life.

[47] Davis 2012.

MDOT’s mission statement reflects the concept of public administration as a balancing act between the interests of the state and rights of the people. MDOT’s main directive is to provide transportation services as a public good. This activity is explicitly recognized as being necessary for *economic activity*, which provides wealth and a tax base to fund the administration of the state. Yet the provision of transportation services is also linked to *quality of life* of Michigan residents. Thus, the Department explicitly considers the preferences and values of Michigan residents in its operational calculus, as illustrated in Figure 4.

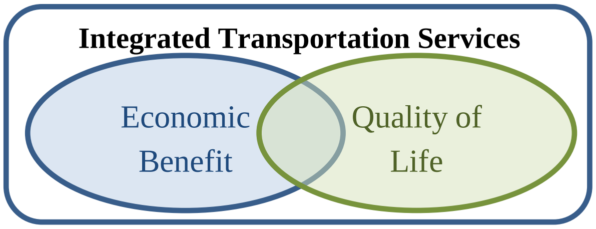

FIGURE 4: VISUAL REPRESENTATION OF THE MDOT MISSION STATEMENT

The values of Michigan residents regarding quality of life may occasionally oppose the provision of an efficient transportation system for raw economic benefit. A classic example may be a highway expansion through an established neighborhood; estimated gains in system efficiency and economic activity may be counterbalanced by the lost value of the current landscape to people who interact with the area. Considering ITS, gains in system efficiency may be counterbalanced by a loss of privacy. There are no easy answers regarding how to strike an appropriate balance. Every project and every decision will have unique ethical implications.

STATE HISTORICAL AND CULTURAL CONSIDERATIONS

Michigan has a history of protecting the individual rights and personal privacy of state motorists. Protecting such rights may often obstruct rational management of the transportation system.

For example, in 1986, Michigan instituted a sobriety checkpoint program, allowing police to establish random checkpoints on public highways. Motorists would be stopped upon reaching the checkpoint and examined by police officers for signs of intoxication. This program was halted by a court order. The Michigan Supreme Court found that sobriety checkpoints violate the Fourth Amendment of the U.S. Constitution and the Constitution of the State of Michigan.[48]

The case was appealed to the United States Supreme Court, which found that the sobriety checkpoints were, in fact, legal by the Fourth Amendment.[49] The U.S. Supreme Court remanded (sent back) the case to the Michigan Supreme Court, which held that Michigan's state Constitution provided greater personal rights than those afforded by the federal Constitution and thus disallowed highway checkpoints within the state.[50] While many states regularly use sobriety checkpoints, they remain illegal in Michigan.

Similarly, Michigan does not allow automated traffic enforcement (e.g., red-light cameras), though many other states do. While not constitutionally restricted, automated traffic enforcement has never been legally permitted.[51] Legislation to allow automated traffic enforcement systems was introduced in 2013 but did not pass out of committee.[52] The bill sponsor withdrew his support, citing privacy concerns.[53]

All considered, Michigan has generally resisted increased monitoring and control of driver behavior.[54] ITS programs that are popularly interpreted as invasions of drivers' rights or privacy may be resisted in Michigan and states with similarly strong traditions of civil liberties, even if such ITS programs promise to improve the safety and/or efficiency of the transportation system.

2.5 CHAPTER SUMMARY

Government employees must often put aside their personal values and consider the ethical principles of the state and agency they are representing. Agencies attempting to enact an ethical ITS data use policy will find very little guidance in legal precedent. For the most part, courts have not addressed ITS technologies deployed for administrative purposes. A transportation

[48] *Sitz v. Department of State Police*. 170 Mich. App. 433 (1988)

[49] *Michigan State Police v. Sitz*, 496 U.S. 444 (1990)

[50] *Sitz v. Department of State Police*. 193 Mich. App. 690 (1992)

[51] Notably, cameras are in no way prohibited on public roads in Michigan. The governing legal requirement is that citation for a moving violation cannot be issued, unless the violation is observed by a "peace officer."

[52] Michigan HB 4763 (2013).

[53] https://www.mackinac.org/19123, accessed February 2014.

[54] While privacy issues have not been a factor, Michigan also has not implemented tollways or vehicle emissions tests.

agency seeking true ethical decision-support must search beneath the legal landscape for the underlying ideals on which our society is founded.

Most of the ethical principles that guide our society are centuries old. In the United States, values that are now considered self-evident can be traced back to figures such as John Locke, Thomas Hobbes, Plato, and Socrates.

The foundational ethics of a society are necessarily interpreted in the current technological, economic, and social context. The founding fathers of the United States, steeped in a classical liberal tradition, were preoccupied with distributing and limiting government power. The idea of a surveillance state would be abhorrent to them. Yet, they could not possibly have conceived of the type of non-obtrusive surveillance that is now possible with contemporary information and communication technology, or the social and political contexts in which we now live.

Transportation professionals are now tasked with determining the appropriate and ethical use of ITS technologies that may include various forms of personal data. The Western philosophical tradition, the American ethos, and the culture of the State of Michigan all suggest that while the government has a valid interest in efficient operation of the transportation system, the privacy of travelers should not be compromised. [55]

[55] It is acknowledged that this Chapter omits vast aspects of classical liberalism and many important figures. This Chapter also does not discuss non-Western influences that are increasingly effecting policy discussions pluralistic societies. The structure of this Chapter was developed by analyzing current debates and literature regarding ITS data ethics, and attempting to deconstruct the arguments into the basic components in order to understand how people have come to adopt various positions on issues that are fundamentally subjective. This Chapter was written in an attempt to provide a minimum amount of contextual and historical information to support the development of the guidelines presented in Chapter 3.

3 ETHICAL GUIDELINES FOR ITS DATA POLICY

Intelligent transportation systems that are legal and effective may nevertheless be ethically undesirable if they are seen as government overreach or an invasion of privacy. It is often unclear when a policy decision requires ethical consideration. Decision-makers in transportation agencies must be relied on to identify when a decision is subject to ethical values, and proceed with appropriate ethical reasoning. This chapter proposes twelve general guidelines intended to provide decision-support to a transportation agency in the design and implementation of an ethically-defensible ITS data policy.

3.1 ETHICAL DECISION POINTS

1. Recognize any use of personally identifiable information as an ethical decision point.

For a state agency to retain public trust while effectively administering public policy, the agency should be proficient at identifying *ethical decision points*. [56] As described by data ethicist, Kord Davis:

> Ethical decision points generate a new type of organizational capability: the ability to conduct an ethical inquiry and facilitate ethical dialog. Such inquiry and discussion is frequently difficult, not only because it comes loaded with people's own personal value systems but also because business historically has not been focused on developing organizational capabilities to facilitate such activities.[57]

In practice, the ability to identify ethical decision points is often informal calls upon our personal sense of morality. Davis has identified this as the "creepy factor. ... This consists essentially of a visceral, almost automatic and involuntary feeling that something isn't quite right. ... It's one of the feelings you can get when what you're experiencing is out of alignment with your expectations."[58]

Identifying an ethical decision point based on 'creepiness' can be useful, but may not be dependable. For ITS data, most ethical decision points concern the

[56] Davis 2012.

[57] Davis 2012. Davis' focus is on the business community, but the discussion regarding ethical decision points is equally applicable to government institutions.

[58] Davis 2012.

collection and use of *personally identifiable location data* (PILD).[59] PILD is a subset of *personally identifiable information* (PII) that may potentially be used to infer the identity of an individual at a location.[60] We often hear of personal data as threatening our privacy, but it is rarely considered what privacy is or why it is of value. In fact, the phrase 'right to privacy' did not exist in U.S. legal discussions until 1890,[61] and it was a technological breakthrough (the camera) that prompted its creation.[62]

The reasons that PII and PILD often prompt a creepy response, particularly in the U.S., can be traced back to the roots of Western liberal democracy. Understanding how the ethical heritage of the United States has influenced our current ideas of privacy will help government agencies formally identify ethical decision points. As discussed in Chapter 2, the United States has a cultural aversion to centralized government power, including the collection and use of personal data. Whenever ITS has the potential to involve PILD, transportation agencies should recognize this as an ethical decision point and consider the matter within an ethical framework.[63]

The remainder of this chapter provides recommended guidelines for decision-support to public agencies handling personally identifiable location data. These guidelines address data creation, data management, and data use.

3.2 DATA CREATION

A critical step in ITS design is to identify what kind(s) of data is needed to meet a defined objective. If the desired data doesn't exist, transportation agencies must determine if they should create it. The focus of ITS data ethics usually centers on *privacy*[64] and especially a person's right to *location*

[59] Garry, Douma, and Simon 2012.

[60] This concept is borrowed from Garry, et al. (2012), who define *personally identifiable location information* (PILI) as, "data that could be used to identify an individual as being at a particular location at a particular time." This report has modified the term and definition because Garry et al.'s definition technically omits potential for privacy breaches in data that does not specify time or has uncertain ability to identify an individual.

[61] Iqbal 2009, 45-78; Warren and Brandeis 1890.

[62] Warren and Brandeis 1890.

[63] Sufficient consideration of ethical issues may often require soliciting public participation in order for an agency to assess normative ethical values of constituents.

[64] *Privacy* is difficult to define. U.S. common law has gradually adopted the Warren and Brandeis (1890) concept of privacy as "the right to be let alone," which is often unhelpful when applied to data privacy.

privacy.[65] Ethical decision points can generally be avoided for ITS that does not incorporate PILD.

PERSONALLY IDENTIFIABLE INFORMATION

2. Avoid the creation of personally identifiable information when a practical alternative exists.

Many researchers suggest that government agencies should only collect the data needed for an identified purpose and use anonymous data whenever possible.[66] Avoiding the creation of PII and PILD may greatly reduce legal liability and ethical indecision.

A common theme in data management is that anonymous data is usually not useful or valuable.[67] However, ITS data is a rare exception. Anonymous data is valuable and sufficient for most mobility, safety, operations, and planning applications.[68]

Deploying ITS that utilizes anonymous data, rather than PII, may also encourage public acceptance of ITS. Some research has suggested that ITS that collect PILD may generate public backlash:

> The negative impact that surveillance has on the autonomy and privacy of individuals sometimes outweighs the benefits. The tension between community trust and the effectiveness ... of surveillance have to be finely balanced.[69]

While ITS may be deployed in the public interest, agencies should consider how such programs will be perceived by the public. It may be appropriate to adopt a broader scope of public interest than transportation agencies usually consider. The deployment of ITS programs that create PILD should be considered carefully. Options that can address policy goals without using PILD should be preferred.

[65] Iqbal 2009, 55 defines *location privacy* as “the interest a motorist has in sustaining a personal location space free from interference by other motorists, telematics providers, and other organizations.” It is important to extend this consideration to non-motorists, as well.
[66] E.g., Cottrill 2013, Ohm 2010, Garry et al. 2012, Douma and Aue 2011.
[67] Ohm 2009.
[68] Garry et al. 2012.
[69] Wigam and Clark, *The Social Impacts of Transport Surveillance*. Prometheus, 24, 2006. referenced in Iqbal 2009.

PRIVACY RIGHTS AND EXPECTATIONS

3. Recognize the ability to travel anonymously as a socially critical ethical value.

In many cases, the benefits of ITS may justify the creation and use of PII and PILD. Indeed, ITS data collection is bound by very few clear legal restrictions and courts have found that people do not have an expectation of privacy on public roads. However, people *do* have some rights to not have their movements tracked.[70] It is not clear how existing case law would apply to location data collected by ITS. Potentially, a transportation agency could legally require users of the transportation system to provide PILD (e.g., through the use of a mandatory transponder), but legal ability does not imply ethical absolution.

When a transportation agency determines that ITS can be deployed without violating peoples' strict legal right to privacy, the agency should still consider the social value of privacy. The regard for privacy on public roads is variable within different contexts. A few examples: users of an automated tolling system generally understand that the toll authority collects PILD; users of connected navigation systems generally understand that they transmit PILD; and states with automated traffic enforcement (e.g., red-light cameras) must collect PILD to issue citations. In these cases, society has accepted ITS that generate PILD. However, in all of these examples, providing PILD is not strictly required to travel from origin to destination: toll-roads can generally be circumvented or paid in cash; connected navigation systems are optional; and automated enforcement cameras (in theory) do not generate PILD unless a traffic ordinance is broken.

The public acceptance of PILD-dependent ITS may require the ability to opt out. The public expectation of privacy in the U.S. is that it should be possible to travel anonymously.[71] As described in Chapter 2, Western democracies have inherited such an ethical value as a rational interpretation of social and

[70] While *U.S. vs. Jones* found that police cannot track a vehicle long term without judicial review, police regularly collect dragnet surveillance data via automated license plate readers. See ACLU 2013.

[71] It is not technically possible to operate a motor vehicle anonymously on public roads, as it requires a license plate; however, absent electronic surveillance we are generally afforded practical anonymity because records of our travels do not exist other than in the sketchy memories of others who observe us. This is discussed in ACLU 2013.

political history. Government agencies should consider the ability to travel anonymously as a socially critical ethical value.

PUBLIC VS. PRIVATE CONTROL OF DATA

4. Pursue partnerships that allow personally identifiable location data to remain in the private sector.

While much ITS PILD is not explicitly collected for law enforcement, there are open questions about law-enforcement's right to access data owned by another public agency. While police agencies would generally need a subpoena or warrant to retrieve such information from private-sector entities, this may not be true for public-sector agencies.[72] Furthermore, data controlled by government agencies is often available for public inspection through federal and/or state Freedom of Information Act (FOIA) laws.[73] The fear that public data could be used by law-enforcement has led to a confusing patchwork of federal, state, and local laws that control government agencies' use of personally identifiable information.[74]

As discussed in Chapter 2, the United States was founded on principles of limited government power. The ethical lineage of Western political philosophy helps explain why many Americans get that *creepy* feeling when government agencies collect data. There is an instinctual fear of government overreach and unchecked police power.

Along with a distrust of government, Americans inherited from the liberal movement a high regard for market economics. People who resist government data collection often freely give-up their PII to private corporations in exchange for some perceived value (e.g., credit card companies and mobile phone service providers). Many people today willingly release large amounts of PII for relatively trivial conveniences or benefits. Many consumers appear to assume that market forces, the legal liability regime, and a sense of

[72] Law-enforcement access to PII held by other public sector agencies is difficult to discuss in general terms. The relationships between agencies can vary greatly, as can state and local statutes that have been enacted to govern this relationship.

[73] While FOIA laws explicitly exempt PII, it can be difficult to determine what is, and is not, PII. Responding to FOIA requests may require agencies to expend significant time and resources determining how to correctly comply with the FOIA while properly protecting PII.

[74] Douma and Aue 2011. Unfortunately, few laws were written with ITS data in mind, so it is difficult to extrapolate ITS data policies from regulatory limitations.

corporate responsibility will ensure that private sector PII is sufficiently protected and will not be used to cause them harm.

Public agencies should consider public-private partnerships that allow the ownership of PILD data to remain in the private sector.[75] This would allow agencies to obtain useful non-PILD data by having access only to data that has been aggregated. The ownership of raw PILD data would remain in the private sector.[76] Law-enforcement agencies would have access to private sector data through established practices of warrant and subpoena. In cases where such a public-private partnership is pursued, the public agency should confirm and verify that the private sector agency has ethically acceptable internal policies regarding PILD data.

INFORMED CONSENT

5. Use informed consent, or opt-in programs, whenever it is necessary to collect personally identifiable location data.

The exchange of PII and PILD for a convenience or service is the basis for many current business models.[77] ITS programs that require PILD may prompt voluntary participation by offering a compelling value proposition. The voluntary and informed consent of people who opt in to providing PILD can provide ethical and legal justification for data use policies.[78] However, it is essential that participants are fully informed about the program with clear privacy policies. People often opt to share their personal information without understanding what is being collected or what it is used for.

Privacy policies are often written "as much to provide cover and protection to [the data collector] ... as they are to protect the consumer."[79] The ethical responsibilities of a state agency require that data use policies are transparent,

[75] MDOT current has multiple contracts with private agencies to obtain data that has been aggregated for use in transportation system administration.

[76] A potential complication to such partnerships is that if a government contractor is hired to perform an action covered by privacy statutes, the contractors may be subject to privacy law to the same extent that the government would be if it had performed that action itself. See, e.g., Privacy Act of 1974, 5 U.S.C. 522a(m)(1). However, it is unlikely that this would prevent governments from purchasing data that would also be available to private sector firms assuming the data meet government privacy requirements.

[77] Cottrill 2013b.

[78] Douma and Aue 2011; Cottrill 2013.

[79] Cottrill 2013.

clear, and protect users from harm. Information that needs to be conveyed to the willing participants usually includes:

- What information is being collected
- How the information will be used
- Who can access personally identifiable information
- The legal consequences for giving consent
- The privacy safeguards that will be put in place over the collected information
- How false information can be corrected
- How long the information will be kept
- Choices to remain anonymous or opt out

In cases where PILD is collected with informed consent, state agencies are still obligated to ensure that the data is unlikely to cause harm to the participant. Research has shown that people often undervalue their own privacy and are generally unaware of the harms that can inflict them by giving up privacy rights.[80] Unlike private sector entities, government agencies have an ethical and constitutional duty to protect the health, safety, and welfare of citizens. Transportation agencies must assure that any PILD collected by ITS is unlikely to cause harm to the participants, even if participants willingly opt in.

3.3 DATA MANAGEMENT AND STORAGE

As discussed in the previous section, ITS programs should try to minimize the creation and use of PII and PILD whenever possible. Once PII exists, it is virtually impossible to guarantee that it will not be used in an unauthorized, unintended, or unethical way. However, some valuable ITS services require PILD. The benefits of ITS may outweigh the risks of PILD data misuse.

There are numerous technological and procedural options to secure data. The data management strategies employed by an agency should correspond to the sensitivity of the data and the amount of harm that may be created by misuse. When ITS data includes PILD, it should be considered highly sensitive and should be secured by appropriate means. Best practices in data security require multiple layers of protection.

[80] Acquisti and Grosslags 2005; Conger et al. 2013.

ACCESS MANAGEMENT

6. Restrict access to personally identifiable information on a need-to-know basis and use best practices in internal data security.

A simple and effective way of protecting PII is to limit data access only to those individuals who require it. State agencies should institute password protection, firewalls, and other best practices as appropriate to minimize the potential for unauthorized access and misuse of the data. Particularly sensitive data should be stored in offline servers when practical to eliminate the chance of unauthorized access ("hacking") through network or internet connections.

ENCRYPTION

7. Encrypt personally identifiable information whenever practical and always when transmitted wirelessly or over public networks.

Substantial security can be provided with *encryption* methods. Encryption is intended to assure that data is not accessed without permission. Generally, encryption adds complexity and cost. Encryption cannot make unauthorized access to data impossible, but best-practices in encryption should make unauthorized access practically infeasible.[81] PII should be encrypted whenever practical. Unencrypted PII should never be transmitted wirelessly.

DATA-SCRUBBING (ANONYMIZATION)

8. Do not rely on data scrubbing alone to protect personally identifiable information.

Existing privacy laws and policies place a heavy emphasis on the use of *data scrubbing* techniques to protect personally identifiable information. Data scrubbing generally refers to removing components of data sets that are used to identify individuals such as names or ID numbers.[82] Unfortunately, recent

[81] Garry et al. 2012. Best-practices in encryption can be very effective, but there are long-term concerns. Researchers are working to develop technologies (i.e., quantum computing) that would negate all current encryption techniques. http://www.washingtonpost.com/world/national-security/nsa-seeks-to-build-quantum-computer-that-could-crack-most-types-of-encryption/2014/01/02/8fff297e-7195-11e3-8def-a33011492df2_story.html, accessed February 2014.

[82] This is often referred to as 'anonymization.' However, Ohm (2011) and others have pointed out that this technique should not be called anonymization because it cannot reliably provide anonymity to users.

advancements in re-identification techniques have reduced the effectiveness of data scrubbing.[83] This is particularly true for PILD.[84] Agencies should use scrubbing wherever practical as part of a PILD data security strategy, but should never rely on data scrubbing alone.

AGGREGATION

9. Use data aggregation techniques whenever possible to minimize use and distribution of personally identifiable information.

Data aggregation provides statistical methods of turning PII into non-PII. A typical example of this is U.S. Census Bureau public data. The Census Bureau collects survey data on individual households. The raw Census data is obviously very sensitive and is protected with a robust and comprehensive data security scheme.[85] The data that is available for public release is aggregated with complex statistical methods to ensure that it cannot be used to infer information about individual people or businesses. When ITS collect PILD, agencies should emphasize the use of aggregated data whenever possible as to minimize access and distribution of the raw datasets.

DATA RETENTION

10. Destroy raw data files containing personally identifiable information as soon as practical.

Considering that digital data storage has become cost-negligible, it may seem beneficial to retain any and all raw data indefinitely as new uses for the data could be developed in the future. However, such future uses may impact privacy or civil liberties. Agencies can reduce the potential for abuse by retaining only anonymous, aggregated data. Any sensitive PII is vulnerable to unauthorized access and unintended use. If PILD must be used for ITS, it should not be archived longer than necessary. Agencies should destroy any PII that is not needed as soon as practical.

[83] Ohm 2011; Narayana and Shmatikov 2008.
[84] Garry et al. 2012.
[85] http://www.census.gov/privacy/, accessed February 2014.

3.4 DATA USE

The legal and ethical considerations in collecting PILD for ITS may depend on the intended use of the data. For ITS that collect PILD, restricting the use of data to administration of the transportation system will reduce the legal liabilities and ethical considerations.

SECONDARY USE

11. Share personally identifiable information only with third parties that can be trusted to use the data as originally intended.

When PII is shared between organizations, it may become difficult to assure that PII is used only as intended and disclosed. The more entities that have access to PII data, the greater the risk of unintended use. Agencies should take care to limit distribution of PII only to organizations that can be trusted to use data as intended and that are capable of preventing unauthorized access.

LAW-ENFORCEMENT

12. Recognize that any data has the potential to be used for law-enforcement, even if this is not the original intent.

The ability to collect PILD for the purposes of law-enforcement has been restricted by court decisions invoking a Fourth Amendment right to privacy.[86] Additionally, when ITS data is used for law-enforcement purposes it often results in an erosion of public trust in government data collection and public opposition to ITS.[87] Transportation agencies have greater legal ability to collect PILD if the intended use is system administration rather than law enforcement. But the rules regarding data sharing between state agencies—such as between DOTs and police departments—are often unclear.

Law-enforcement agencies may be able to access data collected by a public agency without a judicial-review process that would be required if the data were held by a private organization.[88] Furthermore, anti-terrorism laws such

[86] *U.S. v. Jones* (2012).

[87] Wigam and Clark, *The Social Impacts of Transport Surveillance*. Prometheus, 24, 2006. referenced in Iqbal 2009.

[88] For example, *New York v. Burger* (1987) upheld a criminal conviction based on evidence obtained without a warrant, but was obtained during a statutorily-permitted administrative inspection of a junkyard. This ruling pertained to regulated businesses, which have a lower

[CONTINUED ON NEXT PAGE.]

as the *Patriot Act* are often interpreted as over-ruling civil liberty protections. According to one expert, “If the NSA wants [data], there isn’t really any way to stop them.”[89] The control a DOT has regarding data sharing with law-enforcement may be very limited. Legally, a DOT can collect extensive PILD for transportation system administration. Ethically, agencies must recognize that any data has the potential to be used for law-enforcement purposes.

3.5 CHAPTER SUMMARY

This chapter has applied the ethical considerations of government agencies as described in Chapter 2 to contemporary issues of ITS data use. This process resulted in the development of twelve guidelines for an ethical ITS data policy. These are summarized in Table 1 on the following page.

expectation of privacy than individual citizens in their homes. However, since it has been held that individual citizens have very little expectation of privacy on public roads, it seems reasonable that illegal activity discovered in the administration of the transportation system would be held as constitutionally admissible evidence.

[89] Chris Soghoian, Principle Technologist, ACLU. Quoted in http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#Section/1, accessed February 2014.

TABLE 1: TWELVE GUIDELINES OF ETHICAL ITS DATA POLICY

1	Recognize any use of personally identifiable information as an ethical decision point.
2	Avoid the creation of personally identifiable information when a practical alternative exists.
3	Recognize the ability to travel anonymously as a socially critical ethical value.
4	Pursue partnerships that allow personally identifiable location data to remain in the private sector.
5	Use informed consent, or opt-in programs, whenever it is necessary to collect personally identifiable location data.
6	Restrict access to personally identifiable information on a need-to-know basis and use best practices in internal data security.
7	Encrypt personally identifiable information whenever practical and always when transmitted wirelessly or over public networks.
8	Do not rely on data scrubbing alone to protect personally identifiable information.
9	Use data aggregation techniques whenever possible to minimize use and distribution of personally identifiable information.
10	Destroy raw data files containing personally identifiable information as soon as practical.
11	Share personally identifiable information only with third parties that can be trusted to use the data as originally intended.
12	Recognize that any data has the potential to be used for law-enforcement, even if this is not the original intent.

4 REVIEW OF CURRENT AND POTENTIAL MDOT ITS PROGRAMS

This chapter reviews the ethical considerations of specific ITS data that MDOT is currently using or may consider using in the future.

4.1 ADVANCED TRAFFIC MANAGEMENT SYSTEM

The core of MDOT's ITS program is the statewide *Advanced Traffic Management System* (ATMS) administered through regional *Traffic Operations Centers* (TOCs).[90] The TOCs monitor real-time traffic data to deploy MDOT and state police resources.[91] The TOCs also operate *Advanced Traveler Information System* (ATIS) networks that relay transportation system information to travelers and the general public.

MDOT TOCs monitor data from a variety of sources. Three types of ITS data collection equipment are central to this process:

- Closed Circuit Television (CCTV) Cameras
- Microwave Vehicle Detection Systems (MVDS)
- Environmental Sensor Stations (ESS)

MDOT currently maintains approximately 400 CCTV cameras with more planned. Many camera feeds are publicly available on MDOT's *MI Drive* website.[92] Traffic operators use CCTV and MVDS to monitor traffic conditions. The ESS stations also provide valuable weather-related road condition data and can be used to predict potential traffic incidents and possibly mitigate their causes.

None of these current data sources are likely to allow identification of individual vehicles. ESS stations mainly monitor weather. MDOT's MVDS stations record vehicle speeds but do not provide information that could be

[90] The ATMS system operates on a software-as-a-service platform on contract to Delcam Networks.

[91] The combination of traffic operations and law-enforcement agencies within a single operations center has many advantages. The physical proximity between agency employees is intended to facilitate efficient cooperation. However, if traffic operators begin utilizing PILD for system administration, the relationship between traffic operations and law-enforcement may have to be reconsidered.

[92] MI Drive: http://mdotnetpublic.state.mi.us/drive/

used to identify a vehicle.[93] MDOT's CCTV cameras are low-resolution and generally positioned far away from the roadway. It may be possible to interpret general characteristics of a vehicle from the camera feed, but it does not seem likely to be able to identify the license plate or vehicle occupancy.

Further reducing privacy considerations, the video feeds available on MI Drive are not a true live-stream, but still-photos updated every few seconds. Thus there is no guarantee that an individual car would even be captured in the feed.

MDOT traffic operators do have access to live video feeds. But travelers' right to privacy is protected by MDOT's video recording and retention policy. CCTV camera feeds are managed by a third-party contractor and are generally not recorded or archived. MDOT does have some ability to record camera feeds, but is very limited both by policy and system design.[94]

Creating only anonymous visual data, MDOT's ATMS operation seems to be on ethically solid ground. It is difficult to envision any way that MDOT's ATMS data could be used to violate the privacy or civil liberties of travelers.

4.2 TRUCK PARKING INFORMATION AND MANAGEMENT SYSTEM PILOT

MDOT is currently deploying a pilot *Truck Parking Information and Management System* (TPIMS). The MDOT TPIMS is designed to alleviate semi-truck parking overflow issues along the I-94 corridor.[95] The TPIMS program is an innovative ITS solution and an area where MDOT must exercise true ethical judgment. The TPIMS concept of operations is dependent on occasional utilization of closed circuit video cameras for detection accuracy verification. TPIMS video feeds will be available to system

[93] MVDSs report data on aggregated vehicle speed over discrete time bins. Thus, MDOT does not even have access to individual vehicle speeds.

[94] MDOT is capable of connecting one single video stream to a DVD recorder to record the CCTV video. This must be done by physically routing a wire and connecting the video output to the DVD recorder. This process was intentionally built-in to the system in order to make it difficult to record a specific video stream, thus protecting the privacy of travelers.

[95] Castle, Collin. *I-94 Truck Parking Information and Management System Update.* The Intelligent Traveler. January 2013.

administrators, and still-images of truck parking facilities at MDOT rest areas will be publically available on MDOT's MI Drive website.[96]

The use of video surveillance as a component of ITS represents an ethical decision point.[97] Some drivers and trucking agencies may not be comfortable with any application of video surveillance. The public availability of still-images may further decrease perceptions of privacy and anonymity.[98] Drivers may be unaware of the program and thus unable to opt out. Drivers who *are* aware of the program, and wish to opt-out, may have limited alternative options. Finally, the availability of images on the public MI Drive website implies additional privacy and security issues must be considered.

The design of TPIMS has addressed such ethical issues in multiple ways. MDOT and its partners are promoting broad awareness of the program through press releases, signage, and direct engagement with stakeholders. The still-images available on MI Drive are of sufficiently low resolution to make identification of individual vehicles unlikely, and will not even show an entire lot within a single image. While the system will include privately-owned parking facilities, camera images from private lots will not be available on MI Drive. In fact, camera feeds from private lots are unavailable to MDOT staff, as well.[99] Finally, TPIMS does not include any provision for storage of video or image files, and does not in any way collect data on individual persons or vehicles.

MDOT has recognized that the deployment of video surveillance systems in ITS applications must be considered within an ethical framework. MDOT has designed the TPIMS program to minimize impacts on the privacy of drivers and shipping companies while providing a valuable service. As the TPIMS program is evaluated and refined, MDOT and partners should remain aware of the trade-offs involved with using CCTV and other technologies to monitor parking areas, and the impacts on personal and corporate privacy.[100]

[96] I-94 TPIMS Concept of Operations. HNTB and MDOT. August 2012.

[97] See Section 3.1 for more information on ethical decision points.

[98] Alternately, video surveillance of parking areas may give some drivers a greater sense of safety, though the TPIMS cameras are explicitly not a security system.

[99] Camera feeds from private lots are accessible only to MDOT's private-sector partner.

[100] Considerations should include the possible classification of the camera feeds and images as PII. While most people would look at the MI Drive images and see only a number of anonymous trucks, it is possible that some people who are familiar with this trucking route

[CONTINUED ON NEXT PAGE.]

4.3 IN-HOUSE PROBE VEHICLE DATA

MDOT has been dedicated to developing innovative data sources to improve maintenance, operations, asset management, and planning. The department intends to aggregate and synthesize these disparate data sources in the *Data Use Analysis and Processing II* (DUAP II) program. DUAP II will aggregate data from across the organization, but is especially focused on using connected and probe vehicle data.

INTEGRATED MOBILE OBSERVATIONS

MDOT and the University of Michigan Transportation Research Institute (UMTRI) are partnering with the U.S. DOT's Federal Highway Administration (FHWA) on the *Integrated Mobile Observation* (IMO) project. IMO is developing smartphone-based systems to gather road condition data from snowplows and other MDOT vehicles, including PILD. Assuming that the program is confined to MDOT employees during work hours and employees are aware of the process, there does not seem to be substantial ethical concern from a public administration standpoint. Any ethical questions regarding the monitoring of MDOT employees should be properly evaluated and discussed with MDOT managers, employees, and their unions.

VEHICLE-BASED INFORMATION AND DATA ACQUISITION SYSTEM

The DUAP II effort will include a *Vehicle-based Information and Data Acquisition System* (VIDAS) component that will develop tools and methods for collecting road condition data. If the VIDAS program is limited to MDOT vehicles, ethical considerations are generally limited to the relationship between MDOT and its employees.

CROWDSOURCED DATA

There is a potential that MDOT may expand its data collection effort to include the general public. Through a previous research effort, MDOT and CAR concluded that the use of crowdsourced data from smartphones may be an efficient way of obtaining useful pavement condition data for pavement

and the individuals who frequent it would be able to recognize specific trucks and infer the identities of the persons who drive them.

maintenance and asset management.[101] It is premature to consider the ethical implications of such a program in detail because MDOT is not actively pursuing such a strategy at this time.[102]

4.4 RFID TRANSPONDERS

Many agencies have adopted ITS electronic tolling systems for highways and bridges. Automated tolling via *radio frequency identification* (RFID) transponders (e.g., *E-Z Pass*) has made toll collection more efficient both for the individuals and the highway system. The RFID transponders provide location and time data of specific vehicles to the toll authority. Tolling authorities are obligated to protect this data from unauthorized and unethical use. In most cases, drivers may still travel anonymously by paying cash.

If a tolling program is operated by a government entity, it is possible that law-enforcement agencies could legally query RFID tags and set up alerts based on individual license plate numbers. This could be a great help to law-enforcement (for instance, in cases of amber alert or stolen vehicles).[103] However, additional surveillance capabilities for police agencies implies a loss of civil liberties and a potential for abuse. Private tolling authorities would be able to offer users a greater degree of data protection, but PILD would still be subject to subpoena by law-enforcement as well as internal misuse and unauthorized access.

SOCIAL JUSTICE CONSIDERATION OF TOLLING

An interesting ethical consideration of road tolling concerns ‘social justice’ rather than privacy. A great benefit of automated tolling systems is the ability to enact congestion pricing; the toll amount increases with congestion, encouraging users to adjust their travel patterns to minimize impacts. However, research indicates that “lower income motorists are more likely to travel during peak morning hours,” because it is primarily lower income workers who lack the flexibility in their schedule that would allow them to

[101] Dennis et al. *Pavement Condition Monitoring with Connected Vehicle Data*. Center for Automotive Research and Michigan Department of Transportation. January 2014.

[102] MDOT and CAR are further investigating this possibility in a forthcoming report, *Crowdsourcing Transportation Systems Data*.

[103] http://www.michigan.gov/documents/mdot/TF2_RFID_Toll__Road_Program_Overview__254741_7.pdf, accessed February 2014.

avoid rush hour. [104] Thus, congestion pricing is likely to most adversely affect those who can least afford to pay. This is a rare ethical consideration of ITS data that does not center on a right to privacy.[105]

4.5 BLUETOOTH REIDENTIFICATION

It has been estimated that between 5-10 percent of vehicles can be tracked via a Bluetooth device.[106] The share of vehicles containing a Bluetooth device is likely much larger, but the device only broadcasts its median access control (MAC) address while in *discovery mode*. Many Bluetooth devices have a permanent discovery mode, or a user setting that allows this. Only these devices could be reliably tracked.

Bluetooth reidentification can be used to measure arterial travel time, border crossing time, average running speed, and origin-destination patterns of travelers.[107] Some transportation agencies have deployed Bluetooth tracking or purchased the service from a third-party vendor.

Theoretically, Bluetooth probe-vehicle data is anonymous because the MAC address is assigned to a device, not a user. But data-mining techniques can link devices to people. Transportation agencies should manage Bluetooth data as PILD, and should utilize appropriate encryption and security methods. If Bluetooth tracking is contracted through a vendor, MDOT should assure that the vendor's internal ethics and data protection practices meet agency standards.[108]

4.6 AGGREGATED THIRD-PARTY DATA

There are growing opportunities to obtain probe vehicle data from third-party vendors such as navigational services providers,[109] telecommunications data

[104] Lee and Williams 2013.

[105] MDOT is not currently considering congestion pricing or any extensive tolling programs. Further MDOT's legal ability to deploy tolling programs is largely restricted by state and federal regulation.

[106] https://smartech.gatech.edu/bitstream/handle/1853/39597/vo_trung_m_201105_mast.pdf, accessed February 2014.

[107] Cambridge Systematics 2012.

[108] MDOT is currently deploying Bluetooth reidentification to measure border-crossing wait times. Data collection is being done through a private-sector partner, providing MDOT only with aggregated data.

[109] http://www.inrix.com/pressrelease.asp?ID=74, accessed February 2014.

aggregators,[110] and even telecommunications equipment providers.[111] The ubiquity of GPS-enabled smartphones may allow traditional ITS traffic monitoring tools to be augmented or replaced.[112] By 2018, over 75% of the motoring public is expected to own smartphones.[113]

Cell phone users usually obtain service under contracts that promise their personal data will not be distributed. But wireless carriers *are* able to sell or distribute data that has been aggregated, or else 'scrubbed' of personal information.[114] As previously discussed, data-scrubbing cannot be relied on to protect PILD. However, data that is properly aggregated can provide valuable information without compromising privacy.[115]

Wireless carriers or their partners can use PII and PILD obtained through private contracts to provide anonymous and aggregated data to third-party purchasers such as transportation agencies.[116] Agencies may avoid ethical decision points by obtaining such aggregated information from private-sector vendors. To the extent that MDOT pursues this strategy, the agency should verify that the vendor follows internal ethics and security standards.

4.7 U.S. DOT CONNECTED VEHICLE PROGRAM

On February 3, 2013, NHTSA announced an intent to "move forward with vehicle-to-vehicle [V2V] communication technology for light vehicles."[117] NHTSA stated via press release:

[110] http://www.theatlanticcities.com/technology/2012/02/you-already-own-next-most-important-transportation-planning-tool/1124/, accessed February 2014.

[111] One research group obtained access to antennae-level location data from an equipment manufacturer. http://www.theatlanticcities.com/commute/2013/04/aggregating-cell-phone-data-search-pulse-planet/5158/, accessed February 2014.

[112] Leduc 2008.

[113] Dennis and Cregger. *Crowdsourcing Transportation Systems Data.* Center for Automotive Research and Michigan Department of Transportation. Forthcoming 2014.

[114] Private-sector firms are not subject to Fourth Amendment privacy restrictions.

[115] Ohm 2010.

[116] Cellular road traffic data is derived by tracking cellphone tower handoffs. Since the user needs to move between tower ranges to provide data, this technology cannot be used to locate a stationary user with much accuracy. (For more see Cambridge Systematics 2012.) Of course, there are other methods that *can* be used to locate a stationary cell phone with relative accuracy.

[117] http://www.nhtsa.gov/About+NHTSA/Press+Releases/2014/USDOT+to+Move+Forward+with+Vehicle-to-Vehicle+Communication+Technology+for+Light+Vehicles, accessed February 2014.

> NHTSA is currently finalizing its analysis of the data gathered as part of its year-long pilot program and will publish a research report on V2V communication technology for public comment in the coming weeks. ... NHTSA will then begin working on a regulatory proposal that would require V2V devices in new vehicles in a future year, consistent with applicable legal requirements, Executive Orders, and guidance.[118]

The V2V technology expected to be required by NHTSA is likely to be based on the prototype 5.9 GHz *dedicated short-range communication* (DSRC) network being tested in the U.S. DOT Safety Pilot Model Deployment (discussed below). As of July 2014, NHTSA has not yet initiated a formal regulatory procedure, nor specified the role of state transportation agencies. Depending on what role MDOT plays in the management of the national DSRC network, the agency may be involved with the collection and management of large amounts of PILD in real-time and/or in back-office systems.

If a national DSRC network were deployed by federal mandate, it is likely that MDOT would have clear legal and regulatory guidance concerning its role. Data privacy and security of connected vehicles are prime focus areas for the U.S. DOT in the ongoing research and design of the DSRC network. But it is possible that secondary opportunities for data use or ambivalent regulations may still require MDOT to exercise ethical judgment. As with all ITS, MDOT should take care to balance the interests of Michigan residents with those of the agency, private sector interests, and possibly law-enforcement officials.

SAFETY PILOT MODEL DEPLOYMENT

In support of the potential NHTSA connected vehicle regulation described in the previous subsection, MDOT has partnered with the U.S. DOT and others on a public test-bed project for a prototype connected vehicle ITS system in Ann Arbor. The *U.S. DOT Safety Pilot Model Deployment* was designed to collect DSRC connected vehicle data on a publicly deployed test fleet. Various V2V and vehicle-to-infrastructure (V2I) applications are being tested under this program. Data sets collected under this program include:

[118] http://www.nhtsa.gov/About+NHTSA/Press+Releases/2014/USDOT+to+Move+Forward+with+Vehicle-to-Vehicle+Communication+Technology+for+Light+Vehicles, accessed February 2014.

- Basic Safety Messages (BSM)
- Traveler Information Messages
- Signal Phase and Timing (SPaT) Messages
- Geographic Intersection Description Messages

All DSRC messages are relayed from roadside equipment (RSE) units to a back office data management system managed by UMTRI. The foundational message in the V2V system is the BSM. This message is broadcast from each connected vehicle and includes the vehicle's location, speed, and direction.

The storage and management of the BSM logs may impose an ethical concern as they include a vehicle's identity and location.[119] In the pilot study, these concerns are mitigated because drivers volunteered to provide data and are reimbursed for their participation. As long as data use is consistent with the contractual agreement, legal and ethical considerations should be minimal.[120]

4.8 CHAPTER SUMMARY

MDOT's current ITS program does not generally include practices that would suggest a need for ethical reasoning. It is difficult to envision any way that MDOT ITS data could encroach on privacy rights of transportation system users. While CCTV cameras are part of the system, the cameras are of sufficiently low resolution and fidelity to make identification of individual vehicles unlikely. Travelers' privacy is further protected by MDOT's video use policy.

There are a range of ITS tools that MDOT may consider in the future that could include the collection of personally identifiable location data. Such tools may include volunteer probe vehicles, RFID transponders, Bluetooth reidentification, and DSRC connected vehicle data. As per guideline number one, introduced in Chapter 3, any program that uses PILD generates an ethical decision point and requires explicit ethical consideration. MDOT should be conscious of this as it moves forward with ITS planning and deployment.

[119] Volunteers must sign a consent agreement for UMTRI to collect their PILD, which includes the acknowledgement that "It is possible that ... UMTRI could be forced to release data on your driving in response to a court order."

[120] MDOT does not have access to PILD collected through the pilot project. UMTRI and federal researchers are responsible for data analysis.

5 CONCLUSIONS AND RECOMMENDATIONS

This report provides ethical decision-support to transportation professionals in the design and management of Intelligent Transportation Systems (ITS). Existing laws provide almost no guidance regarding ITS data use and related ethical implications. In the absence of legal guidance, public agencies are obligated to use appropriate ethical reasoning to guide ITS data policy. The potential for moral disagreement between individuals requires that agencies seek to establish common ethical principles from which to proceed.

CAR's analysis of the main issues regarding ITS data ethics suggests that formal legal precedent plays a relatively minor role. More influential are the self-evident beliefs of our culture that we have inherited from the Western tradition of ethical philosophy. Ethical discussion surrounding ITS data is usually related to an individual's 'right to privacy.' While this concept did not even enter legal discussions until 1890, the ideals that gave rise to a conceptual right to privacy can be traced back hundreds, even thousands, of years.

CAR analysts used foundational ethical principles as applied to contemporary Western society to develop 12 general guidelines for ethical decision-support in ITS data policy. These guidelines are:

1. Recognize any use of personally identifiable information as an ethical decision point.
2. Avoid the creation of personally identifiable information when a practical alternative exists.
3. Recognize the ability to travel anonymously as a socially critical ethical value.
4. Pursue partnerships that allow personally identifiable location data to remain in the private sector.
5. Use informed consent, or opt-in programs, whenever it is necessary to collect personally identifiable location data.
6. Restrict access to personally identifiable information on a need-to-know basis and use best practices in internal data security.
7. Encrypt personally identifiable location data whenever practical and always when transmitted wirelessly or over public networks.
8. Do not rely on data scrubbing alone to protect personally identifiable information.

9. Use data aggregation techniques whenever possible to minimize use and distribution of personally identifiable information.
10. Destroy raw data files containing personally identifiable information as soon as practical.
11. Share personally identifiable information only with third parties that can be trusted to use the data as originally intended.
12. Recognize that any data has the potential to be used for law-enforcement, even if this is not the original intent.

MDOT's current ITS program does not generally include practices that would suggest a need for ethical concern. It is difficult to envision MDOT's existing ITS creating any data that may result in harm to system users. However, there are a range of ITS tools that MDOT may consider in the future that may include the collection of personally identifiable location data (PILD). Such tools may include volunteer probe vehicles, video surveillance, RFID transponders, Bluetooth reidentification, and DSRC connected vehicle data. As per guideline number one, any program that uses PILD generates an ethical decision point and requires explicit ethical consideration. MDOT should be conscious of this as it moves forward with ITS deployments.

REFERENCES

ACLU (American Civil Liberties Union). *You Are Being Tracked: How License Plate Readers Are Being Used to Record Americans' Movements*. 2013.

Acquisti, Alessandro and Jens Grossklags. *Privacy and Rationality in Individual Decision Making*. 3 IEEE Sec and Privacy 26, 27. 2005. Accessed February 2014 at: http://csis.pace.edu/~ctappert/dps/d861-09/team2-3.pdf

Cambridge Systematics. *Travel Time Data Collection* (White Paper). 2012. Accessed February 2014 at: http://www.camsys.com/pubs/WhitePaper_OD_TTData_Collection.pdf

Conger, Sue, Joanne H. Pratt and Karen D, Loch. *Personal Information Privacy and Emerging Technologies*. Information Systems Journal 23, pp. 401-417. 2013.

Cottrill, Caitlin D. *Considering Smartphones: User attitudes towards trust and privacy in location-aware devices*. TRB 2014 Annual Meeting Compendium of Papers. 2013b.

Cottrill, Caitlin D. *Information Producers, Information Consumers: Location Data Privacy in Institutional Settings*. TRB 2014 Annual Meeting Compendium of Papers. 2013.

Davis, Kord. *Ethics of Big Data: Balancing Risk and Innovation*. O'Reilly Media. September 2012.

Douma, Frank and Sarah Aue. *ITS and Locational Privacy: Suggestions for Peaceful Coexistence*. ITS Institute, Hubert H. Humphrey School of Public Affairs. University of Minnesota. October, 2011. Accessed February 2014 at: http://conservancy.umn.edu/bitstream/116997/1/CTS11-21.pdf

Fukuyama, Francis. *The Origins of Political Order: From Prehuman Times to the French Revolution*. Farrar, Straus and Giroux, New York. 2011.

Gantz, John and David Reinstal. *Extracting Value from Chaos*. June 2011. International Data Corporation (IDC) IVIEW Sponsored by EMC Corporation. Accessed January 2014 at: http://www.emc.com/collateral/analyst-reports/idc-extracting-value-from-chaos-ar.pdf

Garry, Thomas, Frank Douma, and Stephen Simon. *Intelligent Transportation Systems: Personal Data Needs and Privacy Law*. Transportation Law Journal Vol. 39:97. pp. 97-164. 2012.

Hayek, Friedrich. *The Road to Serfdom*. Routledge. 1944.

Hobbes, Thomas. *Leviathan*. 1651.

Hong, Qiang, Joshua Cregger, and Richard Wallace. *Ethics of Government Use of Data Collected Via Intelligent Transportation Systems*. Center for Automotive Research and Michigan Department of Transportation. Ann Arbor. 2012.

Iqbal, Muhammad Usman. *Location Privacy in Automotive Telematics*. School of Surveying and Spatial Information Systems, The University of South Wales. 2009.

Leduc, Guillaume. *Road Traffic Data: Collection Methods and Applications*. Europe Commission Joint Research Center. 2008. Accessed February 2014 at: http://ftp.jrc.es/EURdoc/JRC47967.TN.pdf

Lee, J.F. Jennifer and Jeffrey Williams. *A New Way to Utilize Remote Sensing Data – Automated Road Travel Survey*. UC Davis. 2013. Unpublished draft submitted for consideration to the Journal of the Transportation Research Board on November 15, 2013.

Locke, John. *Second Treatise on Government*. 1690.

Malloy, Robin Paul. *Planning for Serfdom: Legal Economic Discourse and Downtown Development*. University of Pennsylvania Press. 1991.

Mixon Hill. *Advanced Applications of Connected Vehicle Data Use Analysis and Processing*. (DUAP II Concept of Operations) MDOT. v03.0. June 17, 2013.

Nrayanan, Arvind and Vitaly Shmatikov. *Robust De-anonymization of Large Datasets (How to Break Anonymity of the Netflix Prize Dataset).* University of Texas at Austin. 2008. Accessed February 2014 at: http://www.cs.pomona.edu/classes/cs190-2012/netflix_deanon.pdf

Ohm, Paul. *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*. UCLA Law Review, 57. 2010. pp 1701-1777. Accessed January 2014 at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006

Orwell, George. *Nineteen Eighty-Four*. Secker and Warburg, London. 1948.

Plato. *Republic*.

Russell, Bertrand. *The History of Western Philosophy*. London: George Allen and Unwin, 1946.

Scott, James C. *Seeing Like a State: How certain schemes to improve the human condition have failed*. Yale University Press. 1998.

Warren, E. and Brandeis, L. *The Right to Privacy*. Harvard Law Review, 4 pp. 193-220. 1890.

SUPPLEMENTARY BIBLIOGRAPHY

ECONTALK. (Podcast Series) http://www.econtalk.org/

Habermas, Jurgen. *Truth and Justification*. Wiley. 2003.

Locke, John. *A Letter Concerning Toleration*. 1689.

Persig, Robert M. *Zen and the Art of Motorcycle Maintenance.* William Morrow and Company. 1974

philosophy bites. (Podcast Series) http://www.philosophybites.com/

Smith, Adam. *The Wealth of Nations.* 1776.

Smith, Adam. *Theory of Moral Sentiments*. 1759.

APPENDIX A: UPDATED SUMMARY OF 2012 ETHICAL AND LEGAL ISSUES REPORT

CAR's previous report, *Ethical and Legal Issues Facing Government Collection, Management, and Use of ITS Data*, applied content analysis to a broad literature review in the context of the goals and objectives of state transportation agencies in order to generate policy recommendations for agencies and other organizations. The original document provided an overview of legal issues surrounding ITS data collection, management, and use, as well as addressing ethical concerns voiced by MDOT.[1] This summary highlights the major content related to the legal environment, applications, and recommendations related to ITS data and government agencies.

Legal Environment

The United States lacks an overarching information privacy law governing both government agencies and private businesses. In both the United States and Europe, unresolved privacy and liability issues have resulted in slow and fragmented ITS deployment.[2] This section briefly outlines the role of the Fourth Amendment, federal and state laws, and legal decisions relating to ethical use of ITS data.

While individuals widely cite the Fourth Amendment as providing a right to privacy, its implications for ITS and connected vehicle deployment are far from clear. Federal and state laws regulate the collection, management, and use of personal information within government agencies and in some specific industries. Broader issues of privacy and data protection are, however, addressed by a patchwork of legal provisions that has largely been left to individual states and the court system. In the private sector, information privacy protection is largely provided through voluntary self-regulation and use of contracts.

Fourth Amendment Protections

The Fourth Amendment to the U.S. Constitution is the primary basis to claims for a right to privacy in the United States. Although the right to privacy is not

[1] The full 2012 report that was written for MDOT can be accessed via the CAR website at: http://www.cargroup.org/?module=Publications&event=View&pubID=91.

[2] Hoogendoorn, Westerman, and Hoogendoorn-Lanser 2011.

expressly guaranteed in the U.S. Constitution, it has been upheld as a constitutional right as a result of numerous court decisions regarding the Fourth Amendment, which reads:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

The Fourth Amendment protects citizens from unreasonable search and seizure by government officials without due process. A search is constituted by the infringement of an individual's expectation of privacy by a governmental official. Limitations on searches and seizures particularly affects law enforcement agents, and the Fourth Amendment does not apply to the actions of private individuals or businesses.

The Fourth Amendment has been applied to modern technologies and thus protections exist for searches and seizures conducted with the use of electronic devices. Electronic searches and seizures have received significant attention from the courts in recent years.[3]

Federal and State Laws

Privacy law, especially since the 1980s, is largely a response to changes in electronic information technology such as computers, networks, and digital information products. New laws often provide protection against unauthorized use of collected information and government access to private records. In federal laws that are relevant to ITS applications, there is precedent for protecting privacy above and beyond protections offered by the Fourth Amendment.[4]

The Communications Act (1934) established the Federal Communications Commission (FCC) and requires that telecommunications companies protect customer privacy and proprietary information. The FCC is researching privacy and data security practices relating to private information stored on customers' mobile communications devices and how existing privacy and security

[3] These cases have covered the use of new technologies such as electronic beepers, GPS, cellular phone data, and other surveillance technologies, used to track the movement of individuals.

[4] Jacobson 2017.

requirements apply to that information.[5] A regulatory decision resulting from FCC's inquiry could affect connected vehicle service providers in that it may require certain data protections, or may limit what data can be collected and stored using on-board equipment.

The federal Freedom of Information Act (FOIA) of 1966 and similar state FOIA laws require federal and state government agencies to disclose records in their possession upon request. These laws protect the public's right to know and enhance government transparency and accountability.[6] Federal case law has established that drivers do not have a reasonable expectation of privacy while traveling. Therefore, database systems related to ITS data should be designed in a manner that anticipates and resolves problems of access that could result from FOIA requests. Organizations involved with ITS data receive data requests from private and public entities, and FOIA requests are not uncommon.

The Privacy Act (1974) established requirements for federal agencies relating to personally identifiable information. It requires disclosure of the purpose for collecting information, routine uses for the collected data, and consequences for failing to provide requested information. Agencies are also required to establish appropriate security measures to protect privacy. The Electronic Communications Privacy Act (1986) created restrictions on government monitoring of electronic data transmissions and government access to stored communications and telephone communications. The Drivers Privacy Protection Act (1994) prohibits the disclosure of personal information gathered by state Departments of Motor Vehicles and outlines permissible uses of personal driver information. Other laws such as the Communications Assistance for Law Enforcement Act (CALEA) and the Patriot Act have changed how law enforcement officials can monitor individuals. CALEA enhances the ability of law enforcement to monitor individuals by requiring equipment manufacturers and service providers to include monitoring abilities in their products and services. It also enhances electronic communication privacy and places restrictions on obtaining tracking information. The Patriot Act allows federal agencies greater access to electronic data and may allow mobile phone tracking.

[5] Tatel 2012.
[6] National Security Archive 2012 and U.S. DOJ 2012.

Not many state laws address ITS implementation specifically, though some common types of state laws could be relevant for ITS. States with fair information practices statutes restrict the type of personal information that state government agencies can collect, maintain, and disclose. These laws also frequently allow individuals to access and correct information about them held by state agencies. States with statutes regulating wiretaps and stored wire communications restrict state agency access to transmitted and stored information. Some states also have common law remedies which allow individuals to seek redress for invasion of privacy and public disclosure of private information. Supreme Court decisions are not binding on state court interpretations of state constitutional guarantees; therefore, if state protections are greater, state courts may interpret the state constitution freely, regardless of federal rulings.

Court Cases

The case law is relatively clear for simple devices such as beepers used for tracking over short periods of time. However, it is less clear regarding more sophisticated technologies. In general, the courts have ruled that individuals have a decreased expectation of privacy while driving in public and hence have allowed the manual or electronic surveillance and tracking of vehicles on public streets. Some state courts, however, have ruled to require greater restrictions on law enforcement personnel using electronic tracking devices on vehicles.[7] Because cellular and GPS tracking technology can be used to obtain detailed information and present significantly greater capabilities than beeper technology, some argue that it should require higher legal standards.

Many cases involving these newer technologies have referenced cases that involved beepers, with decisions being based off of beeper jurisprudence.[8] In the past few years, courts have come to recognize how much more powerful these newer technologies are. And though the case law is often inconsistent between various state and federal courts, courts commonly require a warrant to use GPS and cellphone tracking technologies.

The Antoine Jones case, decided in early 2012, has led many groups to push for national legislation regulating the use of GPS and cellphone tracking by law enforcement. Some had speculated that the decision could have a broad

[7] Briggs and Walton 2000.
[8] Stephens 2008.

impact on investigative techniques and technologies used by the police, as well as societal expectations of privacy.[9] The Court ruled unanimously that the police needed to obtain an extended search warrant before placing a tracking device on Jones' car, though the majority opinion did not address the capabilities of surveillance technologies, many of which do not require physical trespass by the police. As a result of the ruling, the FBI faced the prospect of turning off 3,000 GPS devices. However, it was able to get warrants for 2,750 of the devices, and thus more than 90 percent of them remained in operation. In those cases for which the FBI cannot get warrants for GPS monitoring, the Bureau is still able to deploy teams to track suspects in person.[10]

Discretion as to how long tracking devices can be used without a warrant is up to future decisions, though the issue has been taken up by legislators in several states, including California, Pennsylvania, Florida, Utah, Minnesota, Oklahoma, Pennsylvania, Utah, and South Carolina.[11] In addition, there have been calls to create national legislation governing the warrant requirements for using GPS tracking devices from groups such as the Constitution Project.[12]

Cell phone tracking has become a commonly used tool in criminal investigations. Police can obtain past billing data kept by mobile providers or more detailed data revealing the minute-by-minute location of a mobile device.[13] In the past few years, there have been several rulings on tracking criminal suspects with satellites and cellphones. In recent years, several high profile cases in state and federal courts had inconsistent rulings with regard to whether a warrant was needed for cellphone and GPS tracking.

Government Agency Policies

The federal government has not adopted a set of privacy policies specifically for ITS applications. However, there has been significant work among federal agencies that considers the issue of privacy. Both the Federal Highway Administration (FHWA) and the National Highway Traffic Safety

[9] MTTLR 2011.
[10] Johnson 2012.
[11] Durkee 2010.
[12] Akey 2013.
[13] McCullaugh 2012.

Administration (NHTSA) have authored reports on connected vehicle technology that outline design goals related to privacy.[14]

FHWA goals are focused on having effective safeguards to prevent data being used for identification of individual vehicles, drivers, or owners. These include vehicle tracking and traffic enforcement applications. In addition, FHWA goals also state that the system's ability to protect consumer privacy should be able to be clearly communicated to the public. NHTSA goals center on security against criminal intrusion or illegal activities. These include intentional tampering or jamming, counterfeiting, identity theft, system circumvention, and unauthorized access to data. NHTSA goals also require mechanisms to detect and reveal transponder negligence, fraud, or cheating. While FHWA and NHTSA list goals for connected vehicle systems, they do not reference formal laws or regulations guiding the design of connected vehicles. In fact, except for the Federal Trade Commission's "Fair Information Practice Principles," there is only limited guidance on privacy issues from the federal government with respect to transportation issues, and none with respect to ITS.[15]

The Michigan Department of Transportation (MDOT) strategic and business plan for deploying connected vehicles, states that ensuring information security is critical, and data exchange will support acceptable standards of user privacy.[16] While the document does not specify privacy standards, it suggests that implementation will require addressing issues related to driver privacy. MDOT has identified driver privacy as a crucial issue and that public acceptance hinges on the adequate protection of civil liberties. That said, MDOT has not yet crafted its own privacy policy for data collected through connected vehicle technology. In 2012, focus group participants identified privacy and security as areas of concern for connected vehicle systems.[17]

Voluntary Commercial Policies

While few laws and policies govern privacy in the design of ITS applications, there are several guidelines for creating ITS privacy policies.[18] Well-known examples include the Intelligent Transportation Systems of America "Fair

[14] Andrews and Cops 2009 and Volpe 2008.
[15] Fries, Chowdhury, and Gahrooei 2011.
[16] Underwood 2008.
[17] Brugeman, Wallace, and Cregger 2012.
[18] Cottrill and Thakuriah 2011.

Information and Privacy Principles"[19] and the "VII Privacy Policies Framework."[20] These documents outline basic principles to govern the design of ITS and connected vehicle systems. They can serve as a starting point for the development of policies addressing regulation on privacy. The documents seek to provide privacy protection for drivers and the principles are designed to be flexible so they will remain relevant despite technological, social, and cultural change. The documents suggest limitations on the acquisition, use, distribution, and retention of data, as well as security and disclosure procedures.

ITS Applications

Privacy implications of ITS technologies are closely related to the types of applications (e.g., safety, operations, and maintenance), selected data collection techniques, and purpose of information collection. There is a broad range of ITS applications and data collection techniques, many of which are currently used by state DOTs or are planned for use in the near future.

Application Categories

The driving forces behind many ITS initiatives are safety and mobility. Most of the applications do not need to specifically identify the travel patterns of an individual vehicle or driver. Therefore, data needs for these applications may not require any personal information or identification. On the other hand, ITS are increasingly used in some emerging applications, such as user-based insurance, road pricing, and vehicle-miles traveled (VMT) fees, which normally require the collection of personal information, including name, address, driver license number, or other personal identifiers, as well as increased accuracy of location data in real-time. The uses of such information could pose a threat to individual privacy.

Data Collection Techniques

The levels of privacy invasion generally depend on what data collection technique is used, what information is collected, how it is stored, and how it is used. For instance, data may be collected using loop detectors, video image detectors, infrared and thermal IR cameras, toll transponders, license plate readers, mobile phones, or probe vehicles. Privacy concerns become even

[19] ITSA 2001.
[20] Jacobson 2007.

more complicated because data may be collected and used by a wide variety of organizations such as telecommunications companies, insurance agencies, government agencies, and private data collection and management firms.

APPENDIX A REFERENCES

Akey, L. (2013). *Requiring a Warrant for Electronic Content Long Overdue, Watchdog Group Says*. Press Release. The Constitution Project, April 25, 2013. <http://www.constitutionproject.org/wp-content/uploads/2013/04/2013.04.25-Requiring-a-Warrant.pdf>.

Andrews, S. and Cops, M. (2009). *Final Report: Vehicle Infrastructure Integration Proof of Concept Executive Summary – Vehicle*. Publication FHWA-JPO-09-003. The VII Consortium. Produced for Research and Innovative Technology Administration, U.S. Department of Transportation.

Baker, R. and G. Goodin. (2011). *Exploratory Study: Vehicle Mileage Fees in Texas*. Texas Transportation Institute, Texas A&M University System. Produced for the Texas Department of Transportation.

Briggs, V. A. and C. M. Walton. (2000). *The Implications of Privacy Issues for Intelligent Transportation Systems (ITS) Data*. Center for Transportation Research, University of Texas at Austin.

Brugeman, V. S., R. Wallace, and J. Cregger. (2012). *Public Perceptions of Connected Vehicle Technology*. Center for Automotive Research. Prepared for the Michigan Department of Transportation. July 2012. <http://www.cargroup.org/?module=Publications&event=View&pubID=92>.

Cottrill, C. and P. Thakuriah. (2011). Protecting Location Privacy: Policy Evaluation. In *Transportation Research Record: Journal of the Transportation Research Board*, No. 2215, Transportation Research Board of the National Academies, Washington, D.C., pp. 67–74.

Douma, F. and S. Aue. (2011). *ITS and Locational Privacy: Suggestions for Peaceful Coexistence*. Center for Transportation Studies, University of Minnesota.

Durkee, M. (2010). Privacy Expectations in the Use of GPS Tracking Devices: United States v. Maynard. *BOLT, Berkeley Technology Law Journal*, November 2010.

Fries, R. N., M. Chowdhury, and M. Reisi Gahrooei. (2011). Maintaining Privacy While Advancing Intelligent Transportation Systems-An Analysis. In *TRB 90th Annual Meeting Compendium of Papers DVD*, No. 1334532, Transportation Research Board of the National Academies, Washington, D.C.

Hoogendoorn, S, M. Westerman; and S. Hoogendoorn-Lanser. (2011). Future Scenarios for Traffic Information and Management. In *Transportation Research Record: Journal of the Transportation Research Board*, No. 2256, Transportation Research Board of the National Academies, Washington, D.C., pp. 79–86.

ITSA. (2001). *Fair Information and Privacy Principles*. Intelligent Transportation Society of America.

Jacobson, L. (2007). *Vehicle Infrastructure Integration Privacy Policies Framework Version 1.0.2*. Institutional Issues SuBCEommittee of the National VII Coalition.

Johnson, C. (2012). FBI Still Struggling with Supreme Court's GPS Ruling. *National Public Radio*, March 2012.

McCullagh, D. (2012). Feds Push for Tracking Cell Phones. *CNET News*, February 2010. news.cnet.com/8301-13578_3-10451518-38.html. Accessed February 16, 2012.

MDOT. (2009). *Transportation Asset Management Data Collection*. Michigan Department of Transportation, 2009.

MTTLR. (2011). United States v. Antoine Jones: GPS Tracking, Privacy Expectations, and Public Places. *Michigan Telecommunications and Technology Law Review*, October 2011.

National Security Archive. (2012). *FOIA Basics*. George Washington University. www.gwu.edu/~nsarchiv/nsa/foia/guide.html. Accessed Feb. 16, 2012.

Newmarker, C. (2007). E-ZPass records out cheaters in divorce court: E-toll devices used to prove cheaters 'took the off-ramp to adultery.' *Associated Press*, August 2007.

Persad, K., C. M. Walton, and S. Hussain. (2007). *Electronic Vehicle Identification: Industry Standards, Performance, and Privacy Issues*. Center for Transportation Research, University of Texas at Austin. Performed for Texas Department of Transportation.

Pethtel, R. D., J. D. Phillips, and G. Hetherington. (2011). *A Policy Review of the Impact Existing Privacy Principles Have on Current and Emerging Transportation Safety Technology*. National Surface Transportation Safety Center for Excellence, Virginia Tech Transportation Institute.

Stephens, C. A. (2008). Caution! Government Intrusion May Be Closer than It Appears: The Seventh Circuit Considers GPS Devices under the Fourth Amendment. *Seventh Circuit Review*, Vol. 3, No. 3, pp. 617-657.

Tatel, J. (2012). Privacy and Security of Information Stored on Mobile Communications Devices. *Federal Register*, Vol. 77, No. 114.

Taylor, B. D. and R. Kalauskas. (2010). Addressing Equity in Political Debates over Road Pricing: Lessons from Recent Projects. In *Transportation Research Record: Journal of the Transportation Research Board*, No. 2187, Transportation Research Board of the National Academies, Washington, D.C., pp. 44–52.

Underwood, S. E., S. J. Cook, and W. H. Tansil. (2008). *Line of Business Strategy for Vehicle-Infrastructure Integration, Part I: Strategic and Business Plan, Vision of Partnership and National Leadership*. Michigan Department of Transportation, 2008.

U.S. DOJ. (2012). *FOIA Resources*. U.S. Department of Justice. www.justice.gov/oip/foia-resources.html. Accessed Feb. 16, 2012.

Volpe. (2008). *Technology Applications for Traffic Safety Programs: A Primer*. Publication DOT-HS-811-040. Volpe National Transportation Systems Center, Research and Innovative Technology Administration, U.S. Department of Transportation. Produced for National Highway Transportation Safety Administration.

APPENDIX B: LIST OF ABBREVIATIONS

ATIS	Advanced Traveler Information System
ATMS	Advanced Traffic Management System
BSM	Basic Safety Message
CAR	Center for Automotive Research
CCTV	Closed Circuit Television
DOT	Department of Transportation
DSRC	Dedicated Short-range Communication
DUAP II	Data Use Analysis and Processing II
ESS	Environmental Sensor Stations
FHWA	Federal Highway Administration
IMO	Integrated Mobile Observations
IP	Internet Protocol
ITS	Intelligent Transportation System
MAC	Median Access Control
MDOT	Michigan Department of Transportation
MVDS	Microwave Vehicle Detector Stations
NHTSA	National Highway Traffic Safety Administration
NSA	National Security Agency
PII	Personally Identifiable Information
PILD	Personally Identifiable Location Data
RFID	Radio Frequency Identification
RSE	Roadside Equipment
SPaT	Signal Phase and Timing
TCP	Transmission Control Protocol
TOC	Traffic Operations Center
TPIMS	Truck Parking Information Management System
UMTRI	University of Michigan Transportation Research Institute
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
VIDAS	Vehicle-based Information and Data Acquisition System
VII	Vehicle-Infrastructure Integration