

Regulating Privacy in Wireless Advertising Messaging: FIPP Compliance by Policy vs. by Design

Heng Xu, John W. Bagby, and Terence Ryan Melonas

College of Information Sciences and Technology
Pennsylvania State University, University Park, PA 16802
{hxx4, jwb7, trm917}@psu.edu

Abstract. This research analyzes consumer privacy issues pertaining to the newly developing wireless marketing context, specifically, wireless advertising messaging (WAM). We develop a conceptual framework named as DIGs (**D**esign innovation/**I**ndustry self-regulation/**G**overnment regulation/**S**tandards) to assess the efficacy of industry self-regulation, government regulation, and technological solutions in ensuring consumer privacy in WAM. In addition to enhancing our theoretical understanding of WAM privacy, these findings have important implications for WAM service providers, mobile consumers, as well as for regulatory bodies and technology developers.

Keywords: Fair Information Practice Principles (FIPP), industry self-regulation, government regulation, privacy enhancing technologies (PETs), architecture design, wireless advertising messaging (WAM).

1 Introduction

The ubiquity of computing and the miniaturization of mobile devices have generated unique opportunities for wireless marketing that could be customized to an individual's preferences, geographical location, and time of day. Unsurprisingly, the commercial potential and growth of wireless marketing have been accompanied by concerns over the potential privacy intrusion that consumers experience, such as wireless spam messages or intrusive location referencing. This research analyzes privacy issues pertaining to wireless advertising messaging (WAM). In this article, WAM is provisionally defined as advertising messages sent to wireless devices such as cellular telephones, personal data assistants (PDAs) and smart phones.

Fair information practice principles (FIPP), the global standards for the ethical use of personal information, are generally recognized as a standard that addresses consumer privacy risk perceptions. Prior privacy literature describes three approaches to implement FIPP: industry self-regulation, government regulation and privacy-enhancing technologies [15, 19]. Industry self-regulation is a commonly used approach that mainly consists of industry codes of conduct and self-policing trade groups and associations as a means of regulating privacy practices. Seals of approval from trusted third-parties (such as TRUSTe) are one example of the mechanism that was created to provide third-party assurances to consumers based on a voluntary

contractual relationship between firms and the seal provider. Government regulation is another commonly used approach for assuring information privacy, which relies on the judicial and legislative branches of a government for protecting personal information [37]. Finally, PETs, also known as privacy-enhancing or privacy-enabling technologies, are broadly defined as any type of technology that is designed to guard or promote the privacy interests of individuals [9]. PET designers often argue that perhaps technological solutions to privacy, although widely implicated for enabling companies to employ privacy invasive practices, could play a significant role in protecting privacy, particularly because of its ability to cross international political, regulatory, and business boundaries, much like the Internet itself [41].

In general, the public has been skeptical about the efficacy of privacy-enhancing technology and industry self-regulation for protecting information privacy [19, 24, 42]. Privacy advocates and individual activists continue to demand stronger government regulation to restrain abuses of personal information by merchants [13, 37]. We seek to contribute to this debate by discussing whether privacy assurance should be better addressed by policy (through industry self-regulation or government regulation) or by design (through privacy enhancing technologies). Toward this end, we develop a conceptual framework named as DIGs (**D**esign innovation/**I**ndustry self-regulation/**G**overnment regulation/**S**tandards) to assess the relative effectiveness of industry self-regulation versus government regulation versus technological solutions in ensuring consumer privacy in WAM. Figure 1 depicts the DIGs framework.

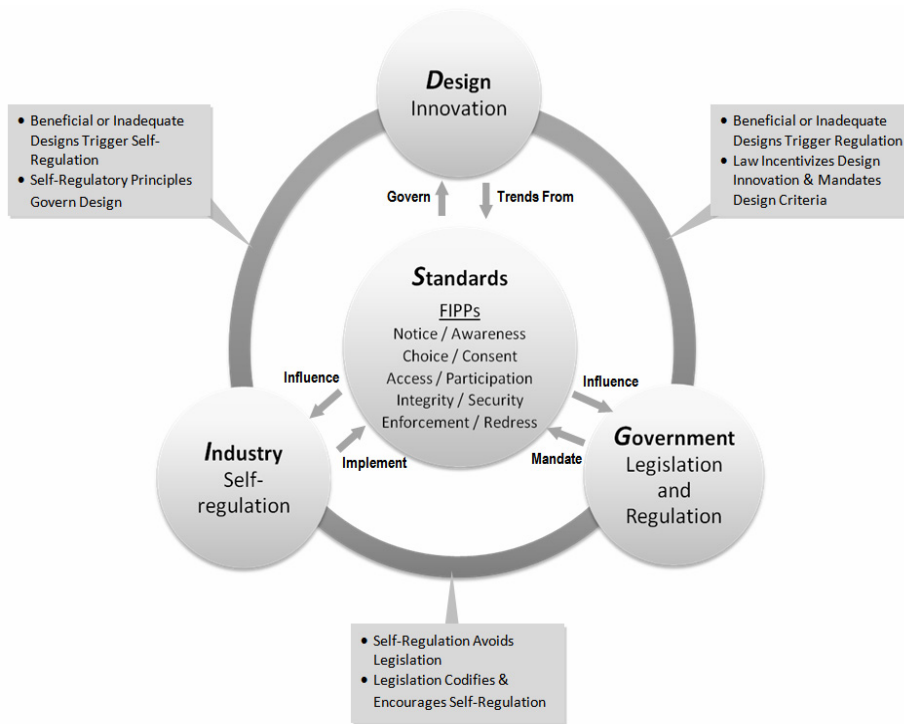


Fig. 1. Conceptual Framework: WAM Privacy by Policy vs. by Design

2 Privacy Standards: The Fair Information Practice Principles

Privacy practices in WAM are subject to a range of standards that purport to protect the privacy of individuals. Among the most notable of these are the “privacy standards” embodied in the Fair Information Practice Principles (FIPP), which originated from a study commissioned by the U.S. Department of Health, Education and Welfare in 1973[30]. FIPP is arguably the first comprehensive treatment of privacy standards that was sufficiently influential to propagate governmental, private-sector and self-regulatory approaches to privacy policy-making. It has been argued that the FIPP have become the de facto global standards for ethical use of personally identifiable information (PII) [29]. However, FIPP are informal, de jure standards that have repeatedly inspired particular mechanisms, rights and procedures in privacy policies including many privacy statutes, regulations and self-regulatory policies that appear in U.S. governmental privacy regulations, in private-sector self-regulatory programs and many other nations privacy public policies (e.g., EU) [3]. Five FIPP are relevant to WAM privacy whether imposed through government regulation, through industry or individual organization/firm self-regulation, arise under contract or result from particular architecture designs. The FIPP include: (1) notice or awareness, (2) choice or consent, (3) access or participation (4) integrity or security and (5) enforcement or redress.

2.1 FIPP Standard No. 1: Notice/Awareness

When applied to WAM, the notice or awareness FIPP standard would alert individuals of the potential for capture, processing and use of their PII. Furthermore, notice could be designed to inform individuals of the purpose intended for the use of their PII. Notice preceding collection of PII would prevent data collection from uninformed individuals. Individuals would be enabled by notice to take counter-measures for protection of their PII before participating in WAM. Furthermore, notice would inform the individual’s choice, including: (i) PII data collector identity, (ii) PII recipient identity, (iii) PII use summary, (iv) PII description if targeted for collection, (v) means and methods expected for collection of PII, (vi) notice when PII collection is pre-condition to subject individual’s participation (e.g., online access, initiating contractual or other relationship with PII collector) and (vii) summary of the information security controls deployed.

2.2 FIPP Standard No. 2: Choice/Consent

The choice or consent FIPP standard would permit individuals to make the final decision to participate in WAM before the collection and use of their PII. This FIPP standard would require the manifestation of consent to be clear and intentional and this consent would need to precede any use of PII in the immediate transaction. Furthermore, consent is necessary before secondary uses of PII, including future “transfers onward” of PII, such as by sale or barter to third parties, an essential design component to most WAM business models. The manifestation of consent ranges through various methods, most notably with either an opt-out or an opt-in. Forthright and full

compliance with this FIPP standard is accomplished when the choice is clear and unequivocal. For example, some WAM architectures would rely on geolocation-based information. This area more strongly suggests the need for clear and unequivocal consent because individuals are subject to more immediate risks if the geolocation PII used in WAM becomes insecure.

2.3 FIPP Standard No. 3: Access/Participation

The third FIPP would enable individuals to review the PII files used in WAM business models in a timely, accurate and inexpensive manner. This standard of access encourages individuals to participate in the assurance of PII accuracy. Without simple and effective means to challenge and correct inaccurate PII individuals' have fewer opportunities to improve PII accuracy that would likely make WAM business models effective. This FIPP standard also illustrates the links among all FIPP: access improves the integrity of PII through personal incentives to audit PII accuracy, thereby enabling security management.

2.4 FIPP Standard No. 4: Integrity/Security

Over a decade of experience now strongly suggests that custodial responsibility over PII has very limited value without close adherence to the fourth FIPP standard: integrity and security. Various government imposed regulation, in the form of statutes, agency regulations, caselaw and standards impose custodial duties on PII database suppliers, owners, customers and operators. These would require WAM participants to assure data quality, assure quality control of data processing methods and thereby safeguard PII from unauthorized access, alteration or deletion. Preventive security under the 4th FIPP deters intrusion. Reactive security under the 4th FIPP must quickly respond to discovered intrusion and effectively remediate the vulnerabilities. Thus, the 4th FIPP requires an adaptive management of continuous improvement of controls that diagnose vulnerabilities as discovered.

2.5 FIPP Standard No. 5: Enforcement/Redress

Many Western societies recognize that rights are hollow without redress. The threat of remedial action against data custodians who are indifferent to the vulnerabilities of subject individual is a powerful incentive towards professionalism. The 5th FIPP standard of enforcement and redress recognizes that duties without correlative rights provide sub-optimal incentives. Therefore, public policy in many Western cultures increasingly relies on some form of enforcement to provide disincentive that closes some of the gaps to shirking by encouraging persistent and quality performance of security-oriented custodial control. Public support is apparently broadening, particularly among victims, to the imposition of enforcement mechanisms that grant remedies for failure of security-related PII custodial duties [20]. The imposition of private rights of action imposing duties enforceable as civil actions for money damages will predictably stimulate opposition from the tort reform movement.

3 FIPP Compliance by Policy: Industry Self-regulation vs. Government Regulation?

As discussed earlier, FIPP are global standards for the ethical use of personal information and are at the heart of U.S. industry guidelines and privacy laws and European Union privacy directives [14]. Complying with FIPP can diminish consumers' privacy risk perceptions through signals that the firm will treat consumers' personal information fairly by addressing procedural, interactional and distributive justice [15]. However, an unresolved issue in this context is *onus* – whether it should be government regulation or industry self-regulation that ensures a firm's implementation of FIPP, and that consumers are accorded legitimate choices about how their personal information is subsequently used [8, 15].

3.1 Industry Self-Regulation or Government Regulation: Privacy as a Commodity or Human Right

The approach for protecting privacy most heavily promoted by industry is self-regulation, which ensures consumers that when they disclose personal information, it will be held in a protective domain wherein a firm becomes a co-owner of the information and accepts responsibility for keeping the information safe and private. The result is that the firm is responsible for managing and protecting the private information by voluntarily implementing privacy policy based on FIPP [15]. Frequently, industry self-regulatory initiatives are reinforced by third party intervention, which involves the setting of standards by an industry group or certifying agency and the voluntary adherence to the set standards by members or associates [15]. An example of an industry self-regulator is the Direct Marketing Association (DMA) that made compliance with its privacy principles as a condition of membership [17]. Other examples include groups such as TRUSTe have been active as third-party entities certifying that participating firms conform to the FIPP they purport to, and acting as a facilitator for resolving any conflicts that may arise [5, 15].

The legislation approach that embodies the strong institutional structural assurances provided by government agencies [44], has been proposed to have a strong impact on protecting consumer privacy [13]. Some scholars have even suggested that the legal system is the most powerful mechanism for addressing privacy issues because it requires that offenders be punished in order to maintain its deterrent effectiveness [35]. With the legal structures in place, illegal behavior can be deterred through the threat of punishment [39]. Thus, recognizing the deterrent value of a legal system, consumers tend to believe that firms would conform to the FIPP as regulated by legislation, and would therefore collect and use personal information appropriately.

The debate between industry self-regulation versus government regulation of FIPP compliance highlights two camps of privacy researchers: those who hold an idealistic interpretation of privacy cannot logically accept that privacy is a pragmatic concept subject to cost/benefit calculus. It is useful to distinguish these two camps by calling the first a fundamental right view of privacy (i.e., "privacy as a human right") and the second an instrumentalist view of privacy (i.e., "privacy as a commodity"). The first

camp views privacy as a fundamental human right, like the right to liberty or life [33, 43]. Such fundamentalist position holds that privacy is tied to a cluster of rights, such as autonomy and dignity [4]. The second camp holds privacy to be of instrumental value rather than fundamental right; that is, the value of privacy comes because it sustains, promotes, and protects other things that we value. In this view, privacy can be traded off because doing so will promote other values (e.g., personalization).

The common theme emerging from current privacy literature is that the distinction between these two camps undergirds much of the dissonance between U.S. and European privacy laws, which is related to (often unstated) assumptions about the validity of “opt in” versus “opt out” information management schema. At the societal level, several studies pointed out that “human right” societies long approached privacy in an “omnibus” fashion by passing sweeping privacy bills that address all the instances of data collection, use and sharing [6, 16, 31]. Some examples of countries in this category include Australia, Canada, New Zealand and countries in European Union [32]. Assigning fundamental rights to personal information would result largely in an opt-in market for information sharing, whereby firms would have access to the information only of those consumers who chose to make it available [31]. In contrast, in “commodity” societies, there are no “omnibus” laws governing collection, use, and sharing of personal information that transcend all types of data in all sectors of the economy [31]. Some countries in this category have “patchwork” of sector-specific privacy laws that apply to certain forms of data or specific industry sectors [6, 16, 31]. For instance, in the U.S., there are sector-specific laws for specific types of records such as credit reports, and video rental records, or for classes of sensitive information such as health information [32]. The “commodity” societies largely see opt-in as an undue burden, thus many would advocate opt-out regimes for protecting consumers’ privacy in which firms collect information unless the consumer explicitly takes steps to disallow it.

3.2 Current State of WAM Industry Self-regulation

The debate between fundamental right versus commodity view of privacy corresponds to the question on the relative effectiveness of industry self-regulation versus government regulation in ensuring WAM privacy. Tang et al. [38] indicates that although overarching government regulations can enhance consumer trust, regulation may not be socially optimal in all environments because of lower profit margins for firms and higher prices for consumers. Nevertheless, skepticism about the effectiveness of industry self-regulation in protecting consumer privacy [e.g., 18, 23] has resulted in privacy advocates and consumers clamoring for strong and effective legislation to curtail rampant abuses of information by firms.

In this section, we describe the current state of WAM industry self-regulation. A number of self-regulatory organizations have developed privacy guidelines that are specifically aimed at wireless advertisers and WAM service providers. While the FTC has encouraged all such regulatory frameworks to abide by FIPP, advertisers who abide by these guidelines may lack comprehensive FIPP coverage. This “a la cart” view of FIPP compliance results in inconsistent regulation across the mobile advertising industry.

The Wireless Advertising Association's (WAA) guidelines for privacy [42] require compliance with all of the FIPP with the exception of enforcement/redress. Advertisers are urged to provide notice of their privacy practices and policy changes to mobile consumers through the use of a privacy policy. In addition, users should be given the ability to decide the types and amount of information that is collected and how that information is used. Wireless advertisers must also obtain opt-in consent before transmitting advertisements or providing a user's PII to third parties. Mobile consumers should be given the ability to opt-out of receiving additional advertisements at any time, and should retain the ability to delete their PII. The guidelines require that advertisers take appropriate steps to ensure that all stored data remains secure [7, 28].

The Direct Marketing Association (DMA), American Association of Advertising Agencies (AAAA), and Association of National Advertisers (ANA), have collaborated to develop a set of email guidelines [17]. It is unclear whether these guidelines apply only to emails sent to mobile devices, or to all advertisements, including those sent using SMS text messages. These guidelines satisfy only the first two FIPP: notice/awareness and choice/consent. Under these principles, email advertisements are required to contain an honest subject line, valid return email address, clear identification of sender and subject matter, and a link to the advertiser's privacy policy. Users should be given clear notice of their right to opt-out of receiving additional advertisements. Opt-in consent must be obtained before an unsolicited commercial email can be sent to a user. A reliable opt-out mechanism should also be included. Email lists should never be sold to third parties without obtaining opt-in consent [28]. These guidelines neglect the remaining three FIPPs.

The Cellular Telecommunications and Internet Association (CTIA) privacy standards [12], known as the "Best Practices and Guidelines for Location Based Services," govern location-based services (LBS). Under these guidelines, LBS providers must supply users with notice of how their location information will be used, disclosed, and protected. Users must be informed of the duration their information will be retained, as well as how third parties may use it. When LBS providers utilize sensitive information, additional periodic notice should be provided. Additionally, LBS providers must obtain opt-in consent before collecting or disclosing location information, and users should be given the ability to revoke this consent at any time. Providers should also employ reasonable safeguards in order to maintain the security of all stored information. Finally, LBS providers should allow users to report abuse or non-compliance with the above principles. These guidelines fail to address two FIPPs, access/participation and enforcement/redress. Users are not given the right to view, alter, or delete their location information.

TRUSTe, a popular privacy certification-granting agency, has developed a set of standards known as the "Wireless Privacy Principles and Implementation Guidelines" [40]. Currently, this is the only set of principles that integrates all five of FIPP's provisions. First, advertisers are required to implement a privacy policy that, if possible, should be displayed every time PII is collected. Mobile users should be notified if the content of this policy is altered. In addition, opt-in consent must be obtained before a

user's PII may be shared with third parties or before location-based information may be used. Advertisers should implement a reasonable mechanism to allow for the correction of inaccurate data. Providers should also take appropriate steps to ensure that all PII is accurate. Under these guidelines, reasonable security measures should be implemented. Finally, an efficient reporting and complaint mechanism should be implemented. While the FTC has struggled to convince private entities to adopt the all of the requirements outlined by FIPP, TRUSTe's guidelines illustrate that FIPP can act as an effective framework.

3.3 Government Regulation

WAM is not clearly and directly regulated under any U.S. federal or state law protecting privacy. Indeed, WAM ostensibly poses a regulatory vacuum with unclear authorities among various state and federal agencies in the U.S. Similarly, the type of optimal enforcement remains unclear so that there are threats but unclear exposures for WAM participants from civil liability, criminal liability and government regulatory agency enforcement (e.g., FTC). The self-regulatory organization (SRO) enforcement efforts are somewhat clearer but generally lack enforcement authority. The precise boundaries of regulatory jurisdiction remain unclear but may hinge on restrictions of the regulatory authority over telecommunications services, such as that of the U.S. Federal Communications Commission (FCC). Furthermore, WAM could be regulated as SPAM or as telemarketing calls [27]. In the U.S. it is important to note that such ambiguity is not fatal to the adaptation of existing government regulations by analogy to various forms of WAM design. For example, the U.S. Federal Trade Commission (FTC) is actively working on WAM regulation but has taken a slow and deliberate pace that has been decidedly *laissez-faire*. The FTC's position explicitly promotes self-regulation, most recently reinforced in the FTC's Behavioral Advertising staff report [21]. Finally, there are proposals to unequivocally regulate WAM and this approach might gain traction if individuals are exposed by WAM to annoyance, injury, identity theft or the like.

4 FIPP Compliance by Design

Proof of FIPP's success or failure as a regulatory framework may be inferred from the existence of FIPP in actual WAM system architectures. It is predictable that WAM service providers will oppose stricter government regulation. Particularly given the FTC's encouragement of the self-regulatory approach, an architecture compliant with FIPP as embodied in self-regulation may preempt government regulation. As a result, system architectures that include effective and innovative FIPP integration are arguably an important component of WAM business models.

FIPP itself may directly influence system design. Lawrence Lessig [25] argues that the hardware, software, and system design that comprises the Internet has a strong regulatory effect. This invisible hand creates a system of governance that can be more effective than traditional forms of regulation. Similarly, much of the regulation that governs WAM may be directly integrated into its architecture. In the U.S., wireless

advertising is still in an embryonic state. In order to take advantage of this new opportunity, many companies are innovating with various business models for delivery of advertisements to mobile users. FIPP is a potentially useful guide for WAM designers who are intent on implementing privacy-compliant solutions. However, if FIPP is not integrated during their initial development, then retroactive compliance will be difficult, and FIPP may never be codified in these architectures.

In a recent statement, Rod Beckstrom, former director of the National Cybersecurity Center expressed his belief that security standards should be directly “baked in” to future network infrastructures rather than being “layered in” after their deployment. Similarly, as various WAM system architectures become entrenched in the market, it is important that they implement the appropriate FIPP compliant privacy provisions up front, rather than as an afterthought or in response to consumer dissatisfaction.

4.1 FIPP Compliance by Design: WAM Patents

Examination of modern WAM architectures reveals the state of FIPP compliance through design. WAM service providers are predictably hesitant to reveal their business models, but alternate design descriptions are available such as through the publication of U.S. utility patents. The U.S. Patent and Trademark Office (USPTO) and other patent services maintain publicly accessible, searchable databases of all issued patents and some patent applications.

Five WAM Patents (see Table 1) are described to examine the FIPP compliance. WAM patents are explored because they proxy major elements of a WAM design and thus are ostensibly good exemplars. These WAM patents were identified using key word in context search methods from among issued U.S. patents. This is clearly a subset of all possible designs for WAM. WAM architectures may include existing designs deployed or announced outside the U.S. Furthermore, the population of WAM patents issued in the U.S. does not include published provisional U.S. patent applications, published full U.S. patent applications, nor any non-U.S. patent or application. A complete WAM architecture may include a combination of elements from WAM patents, existing non-WAM patents, non-patented design elements (e.g., trade secrets) and other public domain elements.

Of the various WAM-related patent documents identified in this survey, the following seven were selected for analysis due to the clarity and relevancy of their architectural descriptions. These patents have elements classified in various USPC classes involving telecommunications, computer communications, business methods, data processing and multiplexing.¹ However, many additional classes and subclasses are likely also relevant to the broader WAM architectures generally envisioned.

¹ This survey largely examines patents classified in various subclasses of one major USPC class: Class 455 Telecommunications. Among the selected WAM patents these additional patent classes are variously claimed: Class 340 Communications: Electrical; Class 370 Multiplex Communications; Class 379 Telephonic Communications; Class 705 Data Processing: Financial, Business Practice, Management, or Cost/Price Determination; Class 707 Data Processing: Database and File Management or Data Structures; and Class 709 Electrical Computers and Digital Processing Systems: Multicomputer Data Transferring.

Table 1. WAM Patents

U.S. Patent No.	Title	Brief Descriptions
6,381,465 (465 patent)	System and Method for Attaching an Advertisement to an SMS Message for Wireless Transmission	A system in which an advertising message is appended to an alert message that a mobile device user registers to receive. Such advertisements would be targeted based on the information that the user entered at the time they registered for the alert, the contextual content of the alert message itself, and the user's location [10].
6,889,054 (054 patent)	Method and System for Schedule Based Advertising on a Mobile Phone	A system for transmitting wireless advertisements to mobile users based on a user defined schedule and personal preferences. Users may also be provided with a reward, such as free "minutes," as an incentive to accept additional advertisements [22].
6,925,307 (307 patent)	Mixed Mode Interaction	A system in which verbal and non-verbal commands are used in conjunction with a mobile device in order to submit search queries and other instructions. Under this system, users have complete control over when and how responses and advertising messages are transmitted. The system also offers a service called a "Voice Wallet," which allows for the storage of sensitive purchasing information, including credit card numbers and expiration dates [26].
7,162,221 (221 patent)	Systems, Method, and Computer Program Products for Registering Wireless Device Users in Direct Marketing Campaigns	A system that allows users to register for targeted, direct marketing campaigns on their mobile devices. After an initial unsolicited advertisement is transmitted, users have the ability to opt-in to participating in the advertising campaign, or opt-out of receiving additional advertising messages [36].
7,251,476 (476 patent)	Method for Advertising on Digital Cellular Telephones and Reducing Cost to the End User	A system in which advertisements are transmitted to cellular phones in a way that does not interfere with the normal operation of the mobile device. The system utilizes a "reverse subscription" model in which advertisers pay users in order to gain permission to send advertisements [11].

4.2 Analysis of FIPP Compliance Using WAM Patents

FIPP is a robust framework that permits analysis of self-regulation or government regulation as well as WAM design. FIPP promotes "Privacy by Policy" and permits the FTC to encourage websites, data collectors, and data processors to integrate FIPP into their privacy policies. This interpretation of FIPP has evolved into a set of standards that influenced the creation and implementation of all forms of privacy regulation, ranging from federal statutes to private self-regulatory frameworks. Spiekermann and Cranor [34] argue, however, that FIPP's "notice" and "choice" principles, arguably two of the most important principles, may not unnecessary if sufficient privacy control is integrated into a WAM system design. Their "Privacy by Architecture" refers to the integration of privacy controls and provisions directly into a system's

design. They argue that system engineers fail to account for privacy when prototyping and developing systems [34]. Nevertheless, technology and system design may be the most effective setting for enforcing privacy regulation.

If FIPP compliance truly adds value to WAM architectures, then those who devise systems that directly integrate FIPP should seek out protection by obtaining a patent. Such protection should further incentivize the development of innovative FIPP implementation strategies. Furthermore, the temporary monopoly granted by patents may facilitate the promotion and universal adoption of a given system. If, on the other hand, such privacy provisions are absent, then FIPP compliance and patent incentives may not have the strength required in order to promote the integration of “Privacy by Architecture.”

FIPP #1: Notice/Awareness. None of the WAM-related patents examined contain any design provisions that satisfy the notice/awareness principle. However, WAM patents openly admit that PII can be collected from users, either with or without their permission. For example, the ‘307 patent [26] describes an advertising system in which all transmitted messages and notifications are based on a user’s personal preferences. Preference information would only be used internally by the WAM service provider. However, the patent fails to describe a method to inform the end user of how this information would be used to provide targeted advertising or how the provider could use the user’s PII in the future. Under the ‘307 patent, users may not be aware that the system maintains a “user profiles database.”

Under the ‘054 patent [22], a large “profile/history” database is maintained. Users may initially assume use of their PII would be limited to their WAM service provider in order to enable the delivery of targeted advertisements. However, without a strict privacy policy or notice provision, this information could potentially be sold or transmitted to third parties without the data owner’s knowledge. Developing unique methods to notify users of the provider’s current privacy practices is especially important within the WAM context. The small screen size of many wireless devices severely limits the amount of space available to effectively communicate a detailed notice statement [24]. Innovative methods to deliver a notification document would likely be rewarded, especially if they were directly integrated into the overall WAM architecture.

FIPP #2: Choice/Consent. Several WAM patents contain opt-in and opt-out provisions for the receipt of advertisements. For example, the ‘476 patent [11] describes a system that is permission-based and only transmits wireless advertisements to users who explicitly opt-in to receiving them. Additionally, under the ‘221 patent [36], advertisers may transmit an initial unsolicited advertising message that allows opt-in to a particular ad campaign, or opt-out of receiving additional advertisements. This system strikes a balance between the privacy interests of the user and the business interests of the advertiser. The ‘307 [26] and the ‘054 [22] patents allow users to determine when, how, and what type of advertisements are received.

Other patents describe wireless advertising systems that do not allow choice. For example, the ‘465 patent [10] automatically attaches advertisements to subscription-based alert messages. Unless the external subscription agreement imposes separate choice for WAM, the ‘465 patent does not envision a permission-based system.

Thus, users registered for specific alerts may be unexpectedly exposed to wireless advertisements. Retroactive imposition of an opt-in or opt-out mechanisms could be imposed when the alert service is registered.

FIPP #3: Access/Participation. None of the patents examined explicitly give users any ability to view, modify, or delete PII stored by the WAM service provider. For example, both the '054 [22] and the '307 [26] patents maintain PII databases based on information that wireless users actively supply to WAM service providers. Nevertheless, neither patent clearly articulates whether this information can be retrieved, altered, or deleted by its owners. Like the discussion above, access might be retroactively supplied, perhaps in an improvement patent.

Even in the patents that do not specifically solicit user preference information, the lack of FIPP #3 access/participation compliance is clear. For example, the '465 patent [10] may use the information that the user inputs when registering for an alert in order to append targeted advertisements to these alert messages. Because such information may be obtained without the user's knowledge, this design fails to provide functionality to view or modify this information once collected. Location information is a key feature of many WAM patents, including the '476 [11], '054 [22], and '307 [26] patents. None of the systems are clearly designed to permit users access to revise or delete their PII.

FIPP #4: Integrity/Security: None of the patents examined in this study contain any security provisions obligating WAM service providers to collect, store, and utilize PII in a secure way. For example, the "Voice Wallet" maintained by the '307 patent [26] may contain critical data, such as a users credit card number, expiration dates, and pin number. Although the "voice authentication" itself is claimed to be secure, there are no patent claims illustrating actual protection of user PII. Moreover, users' preference information may be sent via SMS text message, WML, or voice message, all of which are insecure formats. The '054 [22] system also maintains numerous pieces of critical information, including a "profile/history" database, purchasing information, and shipping information. None of the patent provisions address security maintenance. Many systems, including the '476 [11], '054 [22], and 307 [26] patents, collect and utilize location data, but fail to address the integrity or security of this highly sensitive PII.

Information systems often rely on a series of "standard" information security practices, including data encryption and firewalls, in order to protect the information that they store and process. While these techniques are effective, they are not particularly new or innovative. Such standard security controls might be retroactively applied to business models based on these patents.

FIPP #5: Enforcement/Redress. None of the examined WAM-related patents included any enforcement or redress provision. Enforcement may be viewed as a policy provision rather than a technical constraint exogenous to the design. Here, it is unlikely that the consequences of violating one of the aforementioned self-regulatory principles would be included in a technical system architecture discussion, such as those that are contained in patent documents. Similarly, any possible remedies that may be imposed for such a violation could be included in the subscription agreement, made part of self-regulatory guidelines, or imposed by government regulation. Nevertheless, future WAM system designs could include technical provisions to satisfy the

enforcement FIPP such as automatic recall of PII distributed to third parties or destruction of PII if its collection was unauthorized. Many other alternatives are conceivable, but unexplored in the WAM patents examined for this study.

The WAM-related patents examined here universally fail to comprehensively integrate FIPP. This “al a cart” view of FIPP results in severe privacy inadequacies. Despite these shortcomings, many WAM patents examined here exhibit some form of privacy awareness. As unique and innovative privacy protecting measures are developed, inventors may be incentivized by self-regulation and government regulation to design PII privacy compliant with FIPP. WAM is in its infancy in the U.S., so FIPP privacy compliance is still possible without regulation. The patents examined appear to focus more on providing unique delivery systems rather than FIPP compliance. Once a set of standardized WAM transmission techniques achieve critical mass in the market, developers may seek new methods to differentiate their products. This could include innovative privacy enhancement methods that might better ensure FIPP compliance. The temporary monopolies provided by patents will likely further incentivize these developments if FIPP compliance becomes mandatory.

Unfortunately, under the recent decision of the court in *in re Bilski*, business methods and abstract ideas that are not directly tied to a specific piece of hardware or which do not transform physical matter may no longer be eligible for patent protection. This is the “machine or transformation” test of the *Bilski* case that raises validity questions for most business methods and software patents that operate on general use computers or on standardized platforms. *Bilski* could extend to the WAM-related patents examined here. Thus, the economic incentives to develop innovative FIPP compliance may undermine WAM patents as a major form of system architecture design.

5 Discussion and Conclusion

5.1 Tentative Findings

This research has focused on the following propositions: First, the WAM industry and potential entrants into WAM argue that government regulation would suppress innovation and competition considered socially useful. Second, WAM patents initially appear to provide significant financial reward for WAM innovation. Third, the *Bilski* case and the more general patent reform movement that seeks to limit the impact of business methods patents (BMP) and even software patents more generally, if successful will also suppress WAM innovation.

Several tentative findings from the initial stages of this research lead to the following assertions. Self-regulation and BMP encourage innovation in WAM designs and WAM system architectures. WAM is not directly regulated under any federal privacy, spam or other similar regulatory scheme. The FTC’s current work on location-based services and behavioral marketing has not been clearly merged to adequately address WAM through regulation. The FTC’s deliberate pace has a decidedly *laissez-faire* character that continues to incentivize the development of WAM architectures without close or costly regulation. Indeed, the clear promotion of self-regulation illustrates the nascent WAM industry has some remaining time to address privacy concerns

before the threatened imposition of enforcement or corrective legislation might diminish innovation in WAM architectures.²

WAM poses a regulatory vacuum with unclear authorities among the FTC, FCC, the states, the Justice Department (DoJ). Regulatory uncertainty is exacerbated by ambiguity in the optimal types of enforcement: civil, criminal, regulatory agency, self-regulatory organization (SRO). Regulatory jurisdiction may hinge on boundaries of telecommunications services.³

FIPP is a powerful *de jure* and *de facto* privacy standard and it should continue to inspire any and all government or self-regulation of WAM, however, there is evidence that FIPP is all too often mere rationalization. Opting in vs. opting out, as the satisfaction of the FIPP #1 notice and FIPP#2 choice standards, offer significantly different economic outcomes and costs. The impact of opting form on the size and value of consumer PII databases is also significant clearly incentivizing industries that control the opting scope and method to prefer opt-out over opt-in.

5.2 Future Research Directions

The DIGs framework was proposed in this research to examine FIPP compliance of a few WAM designs as found in WAM patents and the FIPP compliance of various self-regulatory frameworks. This type of analysis should be extended in various ways. First, the patent analysis should be expanded from the current sample of five WAM patents with empirical validation approach. For example, Allison and his colleagues [1, 2] provided some promising methods by working on some large patent datasets, performing patent validity comparisons, analyzing demographic and industrial organization data about inventors, and focusing on particular technology sectors. Second, FIPP compliance is amenable to doctrinal legal and regulatory analysis from various authoritative sources, including *inter alia*: civil litigation among private parties, regulatory enforcement proceedings of various federal agencies engaged in regulation of various WAM components, and criminal violations of various state and federal law. This analysis should address each FIPP separately and then collectively: notice, consent, participation, security enforcement. Results of such analyses are likely discrete given the broad differences between regulatory foci of the agencies in their development of guidelines and rules/regulations, their undertaking of investigations and enforcement and the level of their activity in engagement in “jawboning” with the emerging WAM industry.

The institutional structure of a regulatory domain is of recurring interest to many scholars. For example, the financial crisis of 2008 was marked by very broad public interest in the fragmented regulatory program oversight of the financial services industry. Many of these were the legacy result of Depression-era Glass-Steagall separations of enforcement powers that were specifically intended to spread regulatory powers to avoid regulatory capture, regulatory arbitrage and the financial services monopolization that was experienced during the roaring 20s. Therefore, institutional structural analysis, comparison and prediction are potentially fruitful research avenues.

² FTC Online Behavioral Ad Self-Regulatory Principles at 47.

³ See e.g., 47 U.S.C. §153 (2003).

The sectoral nature of privacy regulation has similar potential for the examination of institutional structure where regulation is fragmented. Consider how WAM architectures immediately implicate telecommunications regulations traditionally within the jurisdiction of the Federal Communications Commission (FCC) but which has been the subject of FTC scrutiny. Additional privacy regulation of the financial transaction components of possible WAM transactions (e.g., automatic crediting of electronic coupons to credit cards, bank accounts or non-bank financial service provider such as PayPal) could be within the regulatory jurisdiction of financial services regulators. Health related advertisements could implicate health needs profiles regulated under HIPAA. Many other WAM architectures and component services could implicate other regulatory programs and other regulators (e.g., children). Research into the optimal regulatory structure is feasible and quite likely to be of interest to various journal readerships.

Finally, a content and stakeholder analysis of the FTC's various dockets in WAM-related areas may be useful. For example, there are sometimes very considerable comment databases accessible online in areas such as behavioral marketing, location-based services, spam, identity theft, data-mining, RFID technology deployments and tracking consumer preferences would be informed by content analysis and of the considerable FTC comment databases.

5.3 Conclusion

Innovation in WAM privacy is incentivized from three major sources: government regulation, industry self-regulation, and privacy enhancing technologies that enable particular WAM market models. Balancing these incentives to improve the security of PII for consumers of WAM services is uncertain because WAM platforms in the U.S. are still under development. WAM is not clearly and directly regulated under any current U.S. law. The prospects for adapting federal privacy law to regulate WAM as a form of spam or telecommunications privacy matter still remains unclear. The FTC's focus on behavioral marketing and location referencing holds the greatest promise for the application of government regulation to WAM. However, the FTC's deliberate pace and laissez-faire approach promotes self-regulation providing there is compliance with FIPP. FIPP has inspired government regulation and industry self-regulation of privacy in various contexts. Furthermore, WAM patents reveal at least some FIPP compliance. However, there is mounting evidence that FIPP is not comprehensively represented in industry self-regulatory programs or in WAM patents. Despite the promise for competitively-inspired innovation to provide privacy-enhancing WAM designs, our examination of industry self-regulation programs as well as WAM patents clearly illustrates that FIPP is not fully implemented. Indeed, the enforcement remedial FIPP is seldom represented and the participation/access of FIPP is lacking in many programs and in issued WAM patents.

It may be useful to examine FIPP compliance in other nations to gain insights. For example, WAM privacy is better established in EU nations so FIPP privacy compliance in the U.S. remains feasible. Other nations' experience can be interpreted to assist WAM policymaking as well as WAM design innovation. WAM privacy resulting from design innovation could be weakened by the invalidity of WAM-related patents, if they are undermined by intellectual property reform such as that in the

recent *Bilski* case. Nevertheless, great insights into the design architecture of WAM services are evident from analysis of WAM patents and such analysis in this article helps pinpoint FIPP non-compliance in design architecture.

Acknowledgments. The authors gratefully acknowledge the financial support of the National Science Foundation under grant CNS-0716646. Any opinions, findings, and conclusions or recommendations expressed herein are those of the researchers and do not necessarily reflect the views of the National Science Foundation.

References

1. Allison, J.R., Lemley, M.A.: Who's Patenting What-An Empirical Exploration of Patent Prosecution. *Vanderbilt Law Review* 53(6), 2099–2174 (2000)
2. Allison, J.R., Lemley, M.A., Moore, K.A., Trunkey, R.D.: Valuable patents. *Georgetown Law Journal* 92(3), 435–480 (2004)
3. Bagby, J.W.: The Public Policy Environment of the Privacy-Security Conundrum/ Complement. In: Park, S. (ed.) *Strategies and Policies in Digital Convergence*, pp. 195–213. Idea Group Reference, Hershey (2007)
4. Beaney, W.M.: Right to Privacy and American Law. *The Law and Contemporary Problems* 31, 253–271 (1966)
5. Benassi, P.: TRUSTe: An Online Privacy Seal Program. *Communications of the Acm* 42(2), 56–59 (1999)
6. Bennett, C.J., Raab, C.D.: The adequacy of privacy: The European Union data protection directive and the North American response. *Information Society* 13(3), 245–263 (1997)
7. Brantley, A.S., Farmer, S.T., Jackson, B.L., Krupoff, J., List, S.S., Ray, E.G.: The Legal Web of Wireless Transactions. *Rutgers Computer and Technology Law Journal* 29(1), 53–88 (2003)
8. Caudill, M.E., Murphy, E.P.: Consumer Online Privacy: Legal and Ethical Issues. *Journal of Public Policy & Marketing* 19(1), 7–19 (2000)
9. Cavoukian, A.H., Hamilton, T.J.: *The Privacy Payoff: How Successful Businesses Build Customer Trust*. McGraw-Hill Ryerson, Toronto (2002)
10. Chern, V., Thorton, K.: System and Method for Attaching an Advertisement to an SMS Message for Wireless Transmission. In: U.S. (ed.) (2002)
11. Cortegiano, M.L.: Method for Advertising on Digital Cellular Telephones and Reducing Cost to the End User. In: U.S. (ed.) (2007)
12. CTIA. *Best Practices and Guidelines for Location Based Services the Cellular Telecommunications and Internet Association (CTIA)* (2008)
13. Culnan, M.J.: Protecting Privacy Online: Is Self-Regulation Working? *Journal of Public Policy & Marketing* 19(1), 20–26 (2000)
14. Culnan, M.J., Armstrong, P.K.: Information Privacy Concerns, Procedural Fairness and Impersonal Trust: An Empirical Investigation. *Organization Science* 10(1), 104–115 (1999)
15. Culnan, M.J., Bies, J.R.: Consumer Privacy: Balancing Economic and Justice Considerations. *Journal of Social Issues* 59(2), 323–342 (2003)
16. Dholakia, N., Zwick, D.: Contrasting European and American approaches to privacy in electronic markets: a philosophical perspective. *Electronic Markets* 11(2) (2001)
17. DMA. *Privacy Promise Member Compliance Guide*. Direct Marketing Association (2003)

18. Edelman, B.: Adverse Selection in Online "Trust" Certifications. Working paper, Harvard University (2006)
19. Fischer-Hüber, S.: IT-Security and Privacy. Springer, Heidelberg (2000)
20. FTC. Federal Trade Commission Report. National and State Trends in Fraud & Identity Theft: January - December 2003 (2004)
21. FTC. FTC Staff Report: Self-Regulatory Principles For Online Behavioral Advertising (2009)
22. Himmel, M.A., Rodriguez, H., Smith, N.J., Spinac, C.J.: Method and System for Schedule Based Advertising on a Mobile Phone. In: U.S. (ed.) (2005)
23. Hui, K.-L., Teo, H.-H., Lee, T.S.Y.: The Value of Privacy Assurance: An Exploratory Field Experiment. *MIS Quarterly* 31(1), 19–33 (2007)
24. King, N.J.: Direct Marketing, Mobile Phones, and Consumer Privacy: Ensuring Adequate Disclosure and Consent Mechanisms for Emerging Mobile Advertising Practices. *Federal Communications Law Journal* 60(2), 229–324 (2008)
25. Lessig, L.: Code: And Other Laws of Cyberspace, Version 2.0. Basic Books, New York (2006)
26. Mandani, M., Johnson, P., Bomar, K., Whatley, T., Grant, C.: Mixed Mode Interaction. In: U.S. (ed.) (2005)
27. Noonan, J., Goodman, M.: Third-Party Liability for Federal Law Violations in Direct-to-Consumer Marketing: Telemarketing, Fax, and E-mail. *The Bus. Lawyer* 63, 585–596 (2008)
28. Petty, R.D.: Wireless advertising messaging: legal analysis and public policy issues. *Journal of Public Policy & Marketing* 22(1), 71–82 (2003)
29. Reidenberg, J.R.: Setting Standards for Fair Information Practice in the U.S. Private Sector. *Iowa Law Review* 80, 497–551 (1994)
30. Secretary. Records, Computers and the Rights of Citizens - Report of the Secretary's Advisory Committee on Automated Personal Data Systems. Secretary of Health, Education, and Welfare (1973)
31. Smith, H.J.: Information privacy and marketing: What the US should (and shouldn't) learn from Europe. *California Management Review* 43(2), 8 (2001)
32. Smith, H.J.: Information Privacy and Its Management. *MIS Quaterley Executive* 3(4) (2004)
33. Sopinka, J.: Freedom of speech and privacy in the information age. *Information Society* 13(2), 171–184 (1997)
34. Spiekermann, S., Cranor, L.F.: Engineering Privacy. *IEEE Transactions on Software Engineering* 25(1), 67–82 (2009)
35. Spiro, W.G., Houghteling, L.J.: *The Dynamics of Law*. Harcourt Brace Jovanovich, New York (1981)
36. Spitz, D., Watkins, D., Cox, S., Thrash, J., Squire, M., Borger, D.: Systems, Method, and Computer Program Products for Registering Wireless Device Users in Direct Marketing Campaigns. In: U.S. (ed.) (2007)
37. Swire, P.P.: Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information. In: Daley, W.M., Irving, L. (eds.) *Privacy and Self-Regulation in the Information Age*, pp. 3–19. Department of Commerce, Washington (1997)
38. Tang, Z., Hu, Y.J., Smith, M.D.: Gaining Trust Through Online Privacy Protection: Self-Regulation, Mandatory Standards, or Caveat Emptor. *Journal of Management Information Systems* 24(4), 153–173 (2008)
39. Tittle, C.R.: *Sanctions and Social Deviance: The Question of Deterrence*. Praeger, New York (1980)

40. TRUSTe. TRUSTe Plugs into Wireless: TRUSTe's Wireless Advisory Committee Announces First Wireless Privacy Standards (2004)
41. Turner, C.E., Dasgupta, S.: Privacy on the Web: An Examination of User Concerns, Technology, and Implications for Business Organizations and Individuals. *Information Systems Management*, 8–18 (Winter 2003)
42. WAA. Wireless Advertising Association Guidelines on Privacy and Spam (2000)
43. Walczuch, R.M., Lizette, S.: Implications of the new EU Directive on data protection for multinational corporations. *Information Technology & People* 14(2), 142 (2001)
44. Zucker, L.G.: Production of trust: Institutional sources of economic structure, 1840-1920. In: Staw, B.M., Cummings, L.L. (eds.) *Research in Organizational Behavior*, pp. 53–111. JAI Press, Greenwich (1986)