

Chapter 2

Individuals' Attitudes Towards Electronic Health Records: A Privacy Calculus Perspective

Tamara Dinev¹, Valentina Albano², Heng Xu³, Alessandro D'Atri⁴, and Paul Hart⁵

¹Department of Information Technology and Operations Management, College of Business, Florida Atlantic University, Boca Raton, FL 33431, USA

²Department of Business Studies, Roma Tre University, Rome, Italy

³College of Information Sciences and Technology, The Pennsylvania State University, University Park, PA 16802, USA

⁴ Late Director of the Research Center on Information Systems (CeRSI), LUISS University of Rome, Rome, Italy

⁵Department of Information Technology and Operations Management, College of Business, Florida Atlantic University, Boca Raton, Florida, USA

Abstract National adoption of Electronic Health Records (EHRs) is considered an essential component of the health care system overhaul sought by policy makers and health care professionals, in both U.S. and Europe, to cut costs and increase benefits. And yet, along with the technological aspects, the human factor consistently proves to be a critical component to diffusion of any IT system, and is even more so regarding health care. The highly personal and sensitive nature of health care data and the associated concerns about privacy impede even the most efficient and technologically perfect system. Our objective is to investigate individuals' attitudes towards EHR and what factors form these attitudes. If we understand individuals' attitudes regarding EHR and the factors that influence them, we will be in a better position to take responsive measure to facilitate Privacy by Design for EHRs. A positivist research model is empirically tested using survey data from U.S. and Italy and structural equation modeling techniques. We find that perceived effectiveness of regulatory mechanisms positively impact trust; perceived effectiveness of technological mechanisms positively impacts perceived privacy

T. Dinev, Ph.D. (✉)

Department of Information Technology and Operations Management, College of Business, Florida Atlantic University, Boca Raton, FL 33431, USA

e-mail: tdinev@fau.edu

control and trust; the latter two help reduce privacy concerns which, along with perceived benefits, convenience, and Internet experience, play the privacy calculus-type formation of attitudes towards EHR.

Keywords Health care • Electronic health care records • Privacy • Attitudes • Structural equation modeling

2.1 Introduction

The health care sector has a significant societal impact, as it affects individuals' quality of life as few other sectors do. Concerns about the quality of health care and economic sustainability have existed for years in all developed economies. Government agencies and business executives who are involved in providing health coverage for workers and citizens have long called for cost control. In United States, a recently published report from the Business Roundtable, which represents CEOs of major companies, has concluded that US health care system has become a liability that hinders companies' competitiveness in a global economy (Alonso-Zaldivar 2009). The unsustainable costs demand system overhaul. As additional twist, the report found that higher U.S. spending fails to deliver a healthier work force, thus creating the largest "value gap" between cost and benefits among the developed economies' health care systems.

While the extent of the value gap is less for the European countries, they also struggle with increased health care costs (Pagliari et al. 2007). Moffit et al. (2001) found that a major factor pushing recent health care policy changes in Europe, including privatization efforts, is the rapid aging of the European population and the stagnated demographics. The unfavorable shift in the demographic balance imposes tremendous financial pressures on the health care and neutralizes the overall higher efficiency of the European nations' health care systems as compared to the United States', thus introducing noticeable urgency for reforms (Moffit et al. 2001).

There is broad agreement that accelerated Information Technology (IT), and specifically Electronic Health Records (EHR) adoption will be critical to close the value gap and reduce the health care costs in general (Landro 2004). Per the definition introduced by Angst and Agarwal (2006a), EHR is a software system that health care providers use to *create, store, update and/or share patient information in electronic format* (see also HHS 2006). Health care is an information-intensive industry, in that a large percentage of its activities are enabled by the storage, processing, transfer, and analysis of data. Quick access to a patient's medical record, often integrated from various sources, can reduce medical errors help diagnosis, and facilitate the communication with related agencies and businesses. Electronic forms and data management, electronic prescription filling, and electronic managed care all increase health care quality and safety, cut costs, and improve efficiency and precision of diagnosis and operations. Thus, digitizing patient records is an essential part of the IT overhaul of the system seeking to improve the care and curbing costs.

Recognizing the importance of the information access and sharing in health care and the slow rate of IT adoption in this sector (Angst and Agarwal 2006a), governments, policy makers, advocacy groups, and individuals have invested extensive efforts to induce more rapid digitization and sharing of medical data both in Europe and North America. In United States, the recently adopted stimulus package dedicates \$50 billion over 5 years to spur the adoption of EHR. In November 2005, the U.S. Senate passed with unanimous consent the Wired for Health Care Quality Act (S. 1418), a bill to enhance the adoption of a nationwide health information technology and to improve the quality and reduce the costs of health care in the United States. In Britain, The NHS (National Health Service), through Connecting for Health, is introducing two types of online health record for everybody in England—the summary care record and HealthSpace (Kidd 2008) that are set to become the world's first fully national system, according to Pagliari et al. (2007). In Italy, a new model of cooperative governance targeting to define national roadmaps coherently with the European guidelines was embraced. The Department of Technological Innovation and the Ministry of Health established an eHealth board called TSE (Tavolo di Sanità Elettronica), charged with coordinated implementation of interoperable IT infrastructures and applications. Since 2005, the TSE has developed a general and comprehensive eHealth conceptual framework and architectural guidelines for a software infrastructure supporting distributed health care processes (TSE 2005, 2006). Coherently with this new approach many projects have been developed fostering the implementation and adoption of new TSE compliant ICT solutions (e.g. the General Practitioners' Network Pilot Program (Rete di Medici di Medicina Generale—RMMG) as well as the interoperability at both national and European level.

Although few question the potential benefits of digitized health care information and it would seem it is ripe and technologically ready for widespread, global adoption, a realistic assessment of the current state of affairs is more sobering. As with every technology, beyond the technical challenges looms the people factor—the individuals' attitudes and readiness to adopt EHR.

There is a significant level of complexity when adoption of EHRs is concerned. On one level, EHR adoption takes place at institutional level: the healthcare provider such as doctors' or dentist's office, a hospital or insurance company adopting a digitized medical record system. It may seem that once the adoption is complete at that level, the patient would not have a choice and would need to automatically comply by letting the provider enter all the necessary medical and personal information in the computer system. However, while patients and individuals cannot directly influence the institutional adoption of a technology such as EHR by healthcare providers, they may resist digitization of their own data until confident that security and privacy policies and practices are in place. As in any case of forcing a technology into individuals, the risk of unintended consequences looms. The importance of the patients' attitudes towards EHRs takes precedence when their weight as political and social capital is considered as an undisputable factor for the success of the nation's transition to electronic healthcare data. Even if providers successfully adopt EHRs, patients can demand to opt-out of digitized

systems, a provision present in all national policies. If controversies and negative attitudes escalate, political pressures may amount to levels that will render any well intentioned policies and institutional and national efforts unachievable. Thus, it is important to understand that patients' cooperation and willingness to allow their medical information in digital form is crucial to the success of EHR (Angst and Agarwal 2009; Bansal et al. 2010).

So far, citizens' attitudes and intentions towards electronic medical systems are not well understood in any country. Angst and Agarwal (2009) point that there is limited knowledge of how patients will be involved in delivery, monitoring, and the dissemination of the information related to their healthcare. However, all the countries that are moving towards the EHRs systems introduce an option for patients to opt-out from having their medical records in electronic form, including Italy and United States. As Angst and Agarwal (2009) point out, patients may demand that their records remain non-digitized (Kauffman 2006) and thus they have a central role in the EHRs diffusion process. The resistance of patients and society in general, the unaddressed and escalating controversies regarding the use of such a sensitive personal information may reach such levels "as to render any national efforts unachievable" (Angst and Agarwal 2009, p. 360). Our study focuses on individual patient's or consumer's attitudes towards EHR as opposed to institutional adoption attitudes by healthcare providers.

As evidenced by many studies, among the major impediments for wide adoption of EHR by patients and consumers are privacy concerns (Angst and Agarwal 2006a, 2009; Bansal et al. 2007; Bodenheimer and Grumbach 2003; Cantor 2001; Earp and Payton 2006; Harris 2002; Masys et al. 2002; Shortliffe 1999; Westin 2003). For example, Bansal et al. (2007) argue that individuals' trust, privacy concern, and information sensitivity are factors in the success of electronic delivery of health services.

Thus, parallel to the efforts for digitization of the health care sector, there is a sense of urgency associated with efforts to ensure strong patient privacy and personal data protection. By focusing on electronic transactions, the privacy regulation required by HIPAA (Health Insurance Portability and Accountability Act of 1996) attempted to assure consumers that as their health records become fully electronic and networked, the information would be protected. Initiatives in the health care sector have led to privacy guidelines and standards for health websites (eHealth) and Health Information Technology (HIT) in general (Choy and Goldman 2001). HIPAA explicitly does not overrule state level privacy rules that often provide stronger protection. It serves instead as a minimum national standard. The core principles and practices of these voluntary efforts are in accordance with the U.S. Federal Trade Commission's (FTC) Code of Fair Information Practices. In Italy, TSE cooperated with the Italian Privacy Authority to the enactment of a set of Privacy Guide Lines on the implementation of an EHR system (Gazzetta 2009), in order to ensure the citizens' control of their personal data. In general, however, self-regulatory efforts differ substantially in focus and comprehension across nations, health care organizations, and providers (Choy and Goldman 2001; Earp and Payton 2006).

In spite of these efforts, many consumers are reluctant to take advantage of the potential benefits associated with electronic health care data due to privacy concerns. The consumers are concerned that misuse of their health information may result in undesirable social or financial consequences (Luck et al. 2006). A recent national study by the California Health care Foundation found that 67 % of the respondents were “somewhat” or “very concerned” about the privacy of their medical records (Bishop et al. 2005). The study also found that recent reports in the media of privacy breaches have raised the level of the concerns, and although consumers are willing to share personal medical information in exchange for better coordination of their medical treatment, privacy protection behavior persists. One in six Americans engages in some form of privacy protective behavior to prevent themselves from a harmful or intrusive use of health information. These privacy protective responses may include: falsify or withhold information; pay out-of-pocket for care; or see multiple providers to avoid a consolidated record; (Rindfleish 1997). Such ‘privacy-protective’ behavior can compromise both individual care and public health initiatives (Lo et al. 1999, p. 3).

It is obvious, then, that the relationships between individuals’ perceptions and behaviors; health care organizations’ policies and practices; their sectors’ guidelines; national regulatory frameworks; and global factors form a complex framework. Individuals—whose acceptance of, and cooperation with, a digitized health care system is critical—form their perceptions from within this complex framework. A fully functional health care IT environment, such as EHR, would lead to individuals’ acceptance only if the individuals first form an overall positive attitude towards that environment. The attitude formation is in its part governed by cost-benefit type of analysis an individual makes about EHR. That is, a positive attitude is formed when positive perceptions outweigh the concerns and risks the individual associates with that environment. Thus, a full understanding of the privacy dynamics regarding the digitization of the health care industry can only be attained by looking across various factors, both positive and negative, that affect the individual’s attitudes towards EHR.

Drawing on attitude and attitude persuasion literatures, Angst and Agarwal (2009) showed that individuals *can* be persuaded to change their attitudes towards EHRs and opt-in behavioral intentions, even in the presence of significant privacy concerns, if appropriate messages about the value of EHR are imparted to the recipient, with argument framing and issue involvement. Angst and Agarwal (2009)’s findings are in accordance with previous research on privacy calculus (Culnan and Armstrong 1999; Dinev and Hart 2006; Laufer and Wolfe 1977) that treated privacy concerns not as acting in isolation, but rather as part of an individual’s cost-benefit analysis in economic, and social contracts. The privacy calculus stream of research showed that high privacy concerns *can* be balanced off by strong positive perceptions about a certain activity that individuals perceive as beneficial (e.g., online shopping, receiving quality health care, etc.). Coming from the rich perspective of privacy calculus, our goal is to identify the factors that, along with privacy concerns, play role in the formation of the overall positive

attitude toward EHR. Thus, our research question is: *What are the factors that drive individuals' attitudes towards EHR?*

While the overarching framework in our study is privacy calculus, we will also be guided by the psychological control theories and trust theories which will help us in the conceptualizations of privacy concerns in the health care context and identify their antecedents and consequences. We argue that perceived privacy control over EHR and consumer trust toward health care providers are two key factors that determine individuals' privacy concerns. We will evaluate the effectiveness of regulatory and technological mechanisms of privacy enforcement on enhancing the perceived privacy control and building consumer trust. We will further investigate how individuals weigh the costs and benefits of potentially compromising some degree of privacy for the possibility of getting better health benefits.

The rest of the paper is organized as follows. We first present the theoretical foundations and develop the conceptual model. Next we discuss the methodology used in this study for the empirical testing of the model. The results and findings are summarized in a discussion section, followed by limitations and suggestions for future research, implications for theory and practice, and conclusion.

2.2 Theoretical Foundations and Research Hypotheses

The proposed research model shown in Fig. 2.1 is anchored in multiple theories. The dependent variable of interest is attitudes toward EHR, and privacy concern is posited as the major factor negatively impacting the attitudes. Attitude toward EHR is determined through an assessment of one's beliefs regarding the consequences arising from use of EHR and an evaluation of the desirability of these consequences (Ajzen and Fishbein 1980). We define the attitude toward digitization of EHR as the individual's positive or negative feelings about providing EHR. We further define *information* privacy concerns (hereafter referred to as privacy concerns) as beliefs reflecting the extent to which individuals are disturbed about the information collection practices of others and how the acquired information will be used (Culnan 1993; Smith et al. 1996; Stewart and Segars 2002).

The overarching theoretical framework for this model is privacy calculus. As a concept, privacy calculus was first considered in the seminal paper of Laufer and Wolfe (1977) and further elaborated by Culnan and Armstrong (1999). Dinev and Hart (2004, 2006) and Xu et al. (2009) developed a quantitative and empirically testable model based on privacy calculus framework. They empirically explored the simultaneous effect of positive and negative personal beliefs, including privacy concerns, all associated with inhibiting or driving behavior or behavioral intention. The set of inhibitors was shown to hinder decisions to get involved in e-commerce transactions. The set of drivers, such as trust and perceived privacy control, was shown to positively influence e-commerce transactions. The important concept in this model is the *cumulative* influence of the inhibitors and drivers, forming the so-called 'privacy calculus' (Culnan and Armstrong 1999)—a mental calculation as to

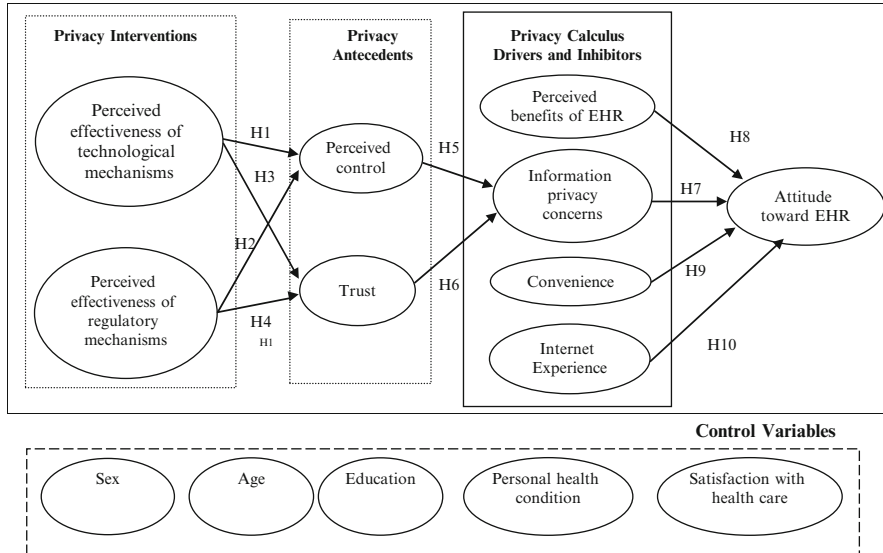


Fig. 2.1 Research model

which beliefs are strong enough to override the contradictory ones. Each set can outweigh the other, determining the user’s final decision on whether to perform a certain behavior or not. If the cumulative effect of the drivers is higher than the cumulative effect of the inhibitors, the user will more likely make a decision to perform the behavior. Otherwise, the behavior is less probable (Chellappa and Sin 2005; Xu et al. 2009).

Dinev et al. (2008) adapted the privacy calculus framework through the lens of the Theory of Planned Behavior (Ajzen 1991) and showed strong and reliable connection between the driving and inhibiting factors and attitudes which in turn are strongly associated with behavior. Thus they argued that attitude formation is also influenced simultaneously by two sets of contrary beliefs. For each individual, these beliefs are weighed and the strength of one may over-ride the influence of another. The relative strength of the inhibitors and the drivers provides insight into a complex process that leads to attitude formation and eventual behavior intention. Higher levels of negative beliefs would suggest individual’s predominant negative attitude that would to resistance to adopt EHR, and vice versa. The fact that our model includes contrary antecedents indicates that their relative influence needs to be taken into full consideration when attempting to understand the resulting attitudes.

To explore the antecedents to privacy concerns relevant in the context of health care, we draw on the theories of psychological control and trust. We hypothesize that the perceived effectiveness of privacy interventions such as the regulatory and technological mechanisms will affect an individual’s perceived privacy control toward EHR and trust toward health care providers.

2.2.1 Privacy Interventions and Perceived Privacy Control Over EHR

The two basic types of privacy interventions in the context of health care and digital medical records are regulation and technology. In this section we posit that the individuals' perceptions of their effectiveness will lead to higher perceived privacy control. Perceived privacy control has been defined as a psychological construct reflecting the belief regarding the extent to which an agent can produce desired outcomes (Skinner et al. 1988, p. 11). One very important psychological perspective views privacy as grounded in the *control* of personal information. For example, Stone et al. (1983) viewed privacy as the ability of the individual to control personally information about one's self. This control perspective of privacy is also found in prior privacy studies that posited that loss of control over information is central to the notion of privacy (Dinev and Hart 2004; Phelps et al. 2000; Sheehan and Hoy 2000). Following this perspective, control (interpreted as psychological control) is identified as one major factor that is closely related to consumers' privacy concerns (Xu 2007; Xu and Teo 2004; Xu et al. 2012). According to Yamaguchi (2001, p. 226), people should feel greater autonomy when they exercise direct personal control, that is, they act themselves as the control agent.

In the health care context, due the heightened concern and perceived risks associated with EHR, privacy interventions—institutional technological and regulatory mechanisms to ensure privacy—have been heavily embarked upon in the design of EHR systems. EHRs are records which may not necessarily be available on the World Wide Web (only providers to access them) but once medical records are digitized, they are practically online. Automatic email generation among providers and to patients will mean that health records are sitting in email servers, routers etc. They can be hacked, used surreptitiously against the individuals and be even more available on the Internet. These risks are very much in people's mind when they think about digital health records and therefore they would want to assert control through control mechanisms. The latter may include ability of individuals to access and modify their own health records or to block others from accessing (and modifying) this information.

A number of technological mechanisms which enhance security of the data and prevent unauthorized use or accidental disclosure (Rindfleish 1997) have been implemented in the recent years. For example, Cimino et al. (2002) proposed to adopt two-factor authentication to enhance user control to their own EHR. In general, the technological trend in the recent years has been to develop tools for the users that will help them enhance their privacy in the EHR. These tools go beyond what is required by policy and security assurances standards the extent of which the users may not be aware of. But small things go long way in that respect. For example, even if policies and mandatory practices do not require it, EHRs may

provide the option for the individuals to control what information he or she will make available to health insurance companies. Do private insurance companies who determine the health insurance premium and out of pocket expenses need to know what contraceptive a woman uses? Or, that 20 years ago someone broke an arm? This is becoming particularly relevant issue given the private insurance exchange markets given in the U.S. health insurance bill. If the users perceive that they have well implemented and effective technological privacy enhancing mechanisms they will feel empowered to exert direct control over their EHR. Hence, they would also perceive they have more control over their EHR. For the purpose of this study, we define perceived effectiveness of privacy enhancing technological mechanisms (for parsimony, also referred to in this paper as perceived effectiveness of technological mechanisms) as the extent to which individuals believe that the privacy protective technologies implemented and used in EHRs are able to provide effective and reliable protection against privacy breaches on their medical data. Therefore, we hypothesize that:

Hypothesis 1: *The perceived effectiveness of privacy enhancing technological mechanisms will lead to higher perceived privacy control over personal EHR.*

When exercise of direct personal privacy control is not readily available or sufficient, people might relinquish their direct privacy control and seek “security in proxy control” (Bandura 1982, p. 142). *Proxy control* is an attempt to gain control through powerful or skillful others when people do not have enough skills, resources, and power to bring about their desired outcome or avoid an undesired outcome (Yamaguchi 2001; Xu et al. 2012). In the health care context, when users perceive that they lack the requisite resources to directly control their EHR, they may reshape their decisions by considering the availability of powerful others (e.g., regulators and legislators) who can act on their privacy preferences. Prior sociology and legal literature lend strong support to the effectiveness of regulatory mechanisms on individuals' control over their personal information (Bandura 1986; Faden et al. 1986). In the health care context, the regulatory mechanism such as HIPAA or country and state-specific laws should be powerful in terms of the exercise of social control (Spiro and Houghteling 1981) since it requires that offenders be punished in order to maintain the deterrent effectiveness of the legal system (Tittle 1980). For the purpose of this study, we define perceived effectiveness of privacy enhancing regulatory mechanisms (for parsimony, also referred to in this paper as perceived effectiveness of regulatory mechanisms) as the extent to which individuals believe that the privacy regulations regarding EHR are able to provide effective and reliable protection against privacy breaches on their medical data.

Hence, viewing the deterrent effectiveness of regulation, individuals would believe that the legal assurance of their privacy control should enable them to exercise proxy control over their EHR. Therefore, we hypothesize that:

Hypothesis 2: *The individual's perceived effectiveness of privacy enhancing regulatory mechanisms will lead to higher perceived privacy control over personal EHR.*

2.2.2 Privacy Interventions and Trust in EHR

Trust is a crucial enabling factor in relations where there is uncertainty, interdependence, risk, and fear of opportunism (Dan et al. 2008; Mayer et al. 1995). Trust has been defined as the willingness to depend on another person or institution based on the belief in the integrity, ability, and benevolence of this other (Mayer et al. 1995; McKnight et al. 2002). In the context of health care, because of security breaches and potential unauthorized or accidental disclosure of sensitive personal medical information (Dixon 2005), there is a heightened risk perception, and the latter is a salient antecedent to any innovative technology acceptance (Xin et al. 2010). Trust comes to be a critical element in helping individuals overcome their perceptions of uncertainty and risk especially in the context of digitization of EHR (Bansal et al. 2010). Similar to Internet and e-commerce trust beliefs, there are several facets of trust in the context of EHR—trust in the healthcare institutions (Doctors' offices, drug companies, insurance companies etc.) that will use EHR (called in the MIS research Institutional trust (McKnight et al. 2002)) and trust in the dependability and reliability of the EHR Information system itself (McKnight et al. 2002). An individual who trusts a health care provider may not necessarily trust EHR systems used by the health care provider. Alternatively, an individual may believe that an EHR information system is well built but the institutions that use and access it may have intentions that are against the interest of the individual. While the complex landscape of the trusting beliefs warrants a separate research and model that will incorporate all the facets of trust, our research is interested in the trust in the EHR systems rather than the trust in the healthcare providers. We also recognize that the two are related—if the healthcare provider effectively implements the privacy enhancing technological mechanisms such as enhanced access control (Cimino et al. 2002), this should directly build individuals' trust beliefs (Hu et al. 2010; Xu et al. 2005) toward a health care provider using EHR. Indeed, a substantial and nontrivial investment of time and resources are required to design and implement the technological privacy-enhancing mechanisms that go beyond the state laws requirements and mandatory protection policies and practices. Such action should be interpreted as a signal that the health care provider is proactively addressing users' privacy concerns and that it will undertake the responsibility to manage users' personal information properly. In other words, effective implementation and use of privacy enhancing technological mechanisms will create user trusting beliefs in the EHR systems used by trusted healthcare providers. Therefore, we hypothesize that:

Hypothesis 3: *The perceived effectiveness of privacy enhancing technological mechanisms will lead to higher users' trust in EHR.*

A health care provider's compliance to and enforcement of the privacy regulatory mechanism should directly build consumer's trust toward the particular health care provider for two reasons. First, the privacy regulatory mechanism could limit the EHR providers' and users' ability to behave in negative or opportunistic ways, allowing patients to form and hold beliefs about expectations of positive outcomes (Johnson and Cullen 2002). Second, when violations do occur, the privacy regulatory mechanism could provide mechanisms of voice and recourse for the betrayed (Johnson and Cullen 2002), which could create strong incentives for health care providers to refrain from opportunistic behavior and behave appropriately and invest the time and resources to build sound, reliable EHR systems. Therefore, we hypothesize that:

Hypothesis 4: *The perceived effectiveness of privacy enhancing regulatory mechanisms will lead to higher users' trust in EHR.*

2.2.3 Perceived Privacy Control and Trust as Antecedents to Information Privacy Concerns

Overwhelming empirical evidence and theoretical arguments reveal that control is one of the key factors that provide the greatest degree of explanation for privacy concerns (Phelps et al. 2000; Sheehan and Hoy 2000; Xu 2007; Xu and Teo 2004). In the e-commerce context, for example, it was shown that individuals have fewer privacy concerns when they have a greater sense that they control the disclosure and subsequent use of their information (Culnan 1993; Culnan and Armstrong 1999; Milne and Boza 1999; Stone and Stone 1990). In this study, we expect a similar negative relationship between perceived privacy control and privacy concerns in the health care context. Therefore, we hypothesize that:

Hypothesis 5: *Perceived privacy control over personal EHR will have a negative effect on privacy concerns.*

The literature on information privacy in the e-commerce context suggests that trust could play an important role in alleviating consumers' privacy concerns (e.g., Caudill and Murphy 2000; Culnan and Bies 2003). Various studies revealed the strong relationship between the two constructs although with various causality direction (Bansal et al. 2007; Dinev et al. 2006). In health care, privacy concerns are a major factor responsible for negative attitudes and resistance to any new way that may risk disclosing personal data. The characteristics of EHR are such that there is an expected increase in the likelihood of privacy violations and misuse of information (Angst and Agarwal 2009). Additionally, the highly sensitive nature of personal medical data adds even more to the uneasiness individuals feel about the violations and misuse. These are general privacy concerns that do not relate to particular systems and practices. People do not want their medical data to land in wrong hands and used against them in any possible way. Whether there will

be security breaches, hacking, or insiders snooping into the personal records for financial, political, or legal gains (for example giving them to the media); whether there will be surreptitious gathering of information by private detectives, insurance companies, or the government to be used in unimaginable and unforeseen for the individuals way, people are uncomfortable with the possible implications of all their records available in one place (rather than folders in various Doctors' offices and hospitals) and used against them. These concerns can never go away completely since they are general and since there so many ways that information can leak. But what can help alleviate them is the trust (a wholesome trust—in institutions and technology) that a particular system, well thought out, well designed and implemented will bring the possibility of such incidents to a minimum. An example of such particular system is EHR.

Based on Hypotheses 3 and 4, we argue that the formation of trust in EHR, by means of the above discussed privacy interventions, will alleviate to a certain extent privacy concerns. If individuals trust their doctors and hospitals in their professionalism and best intentions, they will also trust that the doctors will want reliable, dependable, good EHR systems that will be free of errors, will not be breached, will not be used against the individuals. Therefore, individuals may lower their privacy concerns. We thus view, for the context of EHR in particular, that trust is a necessary precursor that will set the stage for an individual to lower his or her privacy concerns regarding EHR. Without the individual having built trust in the system in the first place, there is no rational for him or her to lower his or her privacy concerns. Therefore, we hypothesize that:

Hypothesis 6: *Trust in EHR will have a negative effect on privacy concerns.*

2.2.4 Drivers and Inhibitors in Privacy Calculus

Information Privacy Concerns

We defined information privacy concerns in the beginning of the theoretical section of this study. As revealed by the cited in the Introduction surveys, the lengths to which consumers will go to hide health information because of privacy concerns are surprisingly great (Bishop et al. 2005). Thus, Angst and Agarwal (2009) argued that the EHR offers a different context than other information technologies with respect to privacy concerns. Following Angst and Agarwal's (2009) arguments, we posit that the multidimensional view of privacy concerns as developed by the Smith et al.'s (1996) concern for information privacy (CFIP) construct is the most appropriate treatment of privacy concerns when digitization of personal medical records and history is concerned. CFIP as composed of four distinct, yet correlated latent factors—(privacy concerns regarding) collection, errors, unauthorized access, and secondary use of information. Stewart and Segars (2002) showed that a second order factor structure is empirically valid and can be used in subsequent empirical models of privacy.

Attitude toward EHR is determined through an assessment of one's beliefs regarding the consequences arising from use of EHR and an evaluation of the desirability of these consequences (Ajzen and Fishbein 1980). Privacy concerns, viewed as a negative antecedent belief, could negatively affect a person's attitude toward EHR. Chellappa and Sin (2005) have similarly argued that when people have stronger concerns about information privacy, their attitudes about using a technology will be more negative, as also confirmed recently by Angst and Agarwal (2009) in the context of EHR. Hence, we hypothesize that:

Hypothesis 7: *Individual's privacy concern will have a negative effect on attitude toward EHR.*

Perceived Benefits of EHR

Perceived benefits are an important component of cost-benefit analysis. IS researchers have utilized perceived benefits as an independent variable that affects adoption of IT innovations (Beatty et al. 2001; Forsythe et al. 2006; MacKay et al. 2004; Teo and Yeong 2003). The literature on perceived benefits points to the important role of this construct in rational decision making. In the context of the research model, perceived benefits are defined as the expected relative advantage associated with using EHR. Analogous to perceived usefulness in the Technology Acceptance Model framework, the perceived benefits are an important antecedent to attitudes (Goodwin 1991; Milne and Gordon 1993). Hence, in the health care context, individuals are more likely to have a positive attitude toward digitization of health care data when they perceive a significant level of benefits in having EHR. Indeed, Song and Zahedi (2007) found that users' beliefs about the ability and benevolence of the health infomediary critically affect their behavior intentions. Therefore:

Hypothesis 8: *Perceived benefits of EHR will have a positive effect on attitudes toward EHR.*

Convenience

Convenience has been considered in e-commerce transactions as a utilitarian motivator that positively affects attitudes and behaviors of consumers (Childers et al. 2001). Convenience is defined as the individual's perception of presence of a set of opportunities that facilitate the accomplishment of a task, and also make the process of accomplishing the task more appealing. The convenience in interactive use of medical records increases search efficiency through the ability to do that at home (Angst and Agarwal 2006a, b), by eliminating such frustrations as fighting traffic and looking for a parking space, and avoiding long lines at medical offices for simple documentation handling, scheduling appointments, or gathering recent test results from various offices. Convenience is manifested in the single

“stop” for all your medical records (Angst and Agarwal 2006b) that eliminates travel to and from a variety of offices and long telephone tags with the doctors, clinics, and insurance companies. Thus, convenience includes both the elements of when and where a patient can operate with his or her medical records. Indeed, speed, efficiency, ease of finding the information or performing tasks 24/7 increase substantially the advantage and uniqueness, as was shown in the case of online shopping (Childers et al. 2001). We should expect the same relationship to be valid for EHR as well, as also found by Angst and Agarwal (2006b). Indeed, the convenience of the medical clinical data to be available electronically: the patients and their doctors and pharmacists to pull them fast and error-free when needed, without the risk of loss or misplacement, are all pointing to the high utilitarian value of EHR. Therefore:

Hypothesis 9: *Convenience will have a positive effect on attitudes toward EHR.*

Internet Experience

Significant extant research has shown that technology experience can affect attitudes towards the various technologies (e.g. Taylor and Todd 1995; Venkatesh et al. 2003). Experience and continued usage of technology informs the individual’s expectations about its capabilities, benefits, and drawbacks, as well as his or her familiarity with that technology. Through greater experience and familiarity, individuals form more positive reactions to new technologies (Bansal et al. 2007; McKnight et al. 2002). Relating these findings to the context of EHR which is an online technology, we posit that Internet experience and frequent internet shopping will help to build positive attitude formation towards EHR. Therefore:

Hypothesis 10: *Internet experience will have a positive effect on attitudes toward EHR.*

Control Variables

Based on prior research on adoption and consumer behavior, a number of additional factors may influence privacy concern, trust, and attitudes toward EHR. Because there is no sufficient theoretical argument that we can draw on to include them in our model as antecedents, we include them as control variables, to eliminate the variance explained by them. They are *sex, age, education, personal health condition, and satisfaction with health care.*

2.3 Research Methodology

2.3.1 Construct Operationalization and Scale Development

Most of the measurement items of the survey instrument were adapted from extant instruments in the literature (Table 2.1) and a pilot study was conducted to test for clarity, consistency, and validity with 27 undergraduate and graduate students in a Southern U.S. university acquainted with EHR. Following standard practices, scales were purified and refined. In general, however, the pilot test resulted in only minor changes to the initial instrument. Several items were dropped for parsimony of the model (Pavlou and Fygenson 2006). The instrument is given in the Appendix.

2.3.2 Data Collection

Since the issues discussed in this study are truly global, the researchers sought to eliminate U.S. biased treatment of the theory and the findings, with this enhancing the generalizability of their model by collecting data from U.S. and Europe. With this we believe that the implications of the model will inform in a more convincing way the policy makers, health care executives and providers and transcend national specifics of the health care model. The researchers chose Italy as a typical European style of health care provider—by and large, the Italian government provides universal health care and is committed to implementing electronic health care records in the nearest future. Since the health care model in most European countries

Table 2.1 Sources of construct operationalization

Construct	Source of measurement items
Attitude toward EHR	Pavlou and Fygenson (2006), Taylor and Todd (1995)
Convenience	Angst and Agarwal (2006a)
Perceived privacy control over HER	Xu (2007)
Privacy concerns—collection, errors, unauthorized access, secondary use	Angst and Agarwal (2009)
Perceived benefits	Iacovou et al. (1995), Liu (2007)
Perceived effectiveness of regulatory mechanisms	Pavlou and Gefen (2004), Xu et al. (2008)
Perceived effectiveness of technological mechanisms	Xu et al. (2008)
Trust	Jarvenpaa et al. (2000); McKnight et al. (2002); Pavlou and Fygenson (2006)
Health status	Bansal et al. (2007)
Experience with internet	Angst and Agarwal (2006b), Bansal et al. (2007)

is substantially different from the one in US, we introduced a control variable, satisfaction with current health care, to capture the citizens' attitudes towards their current health care system, and to eliminate possible influences if differences exist. To ensure that the subjects understand the use of the term and the nature of EHRs, we provided detailed description of the systems and how they can be used by the doctors and by the patients. The questionnaire was translated from English to Italian by native Italian speakers and then back to English following a generally accepted practice to ensure consistency in cross-lingual surveys (Karahanna et al. 2002). It was pretested with multiple respondents from Italy and U.S. with diverse age, gender, and education. While no major problems were identified, instrument was further refined and a few modifications in the Italian translation were made.

The goal in the data collections from both countries was to reach as diverse sample as possible that would closely follow the representation of the demographic categories of the general population. For that purpose, individuals were approached in various settings, including hospital and doctors' waiting rooms, neighborhoods, small business and public meeting places such as parks and transport stations. The individuals were asked to participate completely voluntary and if they wished, a preaddressed and prepaid envelope was given to them, so they can fill in and return the survey by mail at a later time. After eliminating several responses due to multiple empty entries, we used total of 217 responses from United States and 188 from Italy. The demographic distribution (Table 2.2) shows that both Italian and U.S. samples are diverse, comprising a wide range of age, education, with equal representation of genders.

2.3.3 Model Testing

The model developed in this study (Fig. 2.1) was tested by Structural Equation Modeling's (SEM) Partial Least Square (PLS) Method using SmartPLS 2.0 (Ringle et al. 2005). A two-stage approach, as recommended by Gefen et al. (2000), was used to first assess the quality of the measures through the confirmatory factor analysis (CFA) stage and then test the hypotheses through the structural model, the SEM stage. The CFA was performed on the entire set of items simultaneously with each observed variable restricted to load on its a priori factor. Validation and reliability assessment of the measurement model were conducted following the widely used SEM heuristics Gefen et al. (2000).

Measurement Model

The measurement model was assessed for the following three criteria: (1) item reliability and convergent validity, (2) internal consistency, and (3) discriminant validity. The factors loadings of the measurement items are presented in Table 2.3. To assure measurement adequacy for both nations, we ran the measurement model separately

Table 2.2 Demographic characteristics of the Italian and U.S. samples

	Sex	Age			Education			Graduate degree	Bachelors degree	Some college degree	GED or equivalent	Knowledge of EHR		Health status		Satisfaction with current health care		Internet experience		
		<30 years	30-60 years	>60 years	High school or less	High school	GED or equivalent					Mean (Std Dev)	Mean (Std Dev)	Mean (Std Dev)	exp1	exp2	exp3			
Italy	98	90	64	86	38	13	53	17	34	34	71	1.74 (.99)	3.41 (.88)	2.85 (1.13)	1.81 (1.18)	2.32 (1.46)	2.86 (1.46)			
U.S.	119	98	82	78	41	59	57	9	45	47	47	1.71 (1.08)	3.17 (1.11)	2.99 (1.43)	2.97 (1.43)	4.00 (1.23)	4.10 (1.28)			

Notes: Knowledge of EHR: How much are you informed about the EHR (Not at all—Very well)

Table 2.3 Item loadings and cross-loadings, Italy and U.S.

	Italy															U.S.														
	ATT	CO	CTRL	LIKE	PCON	PERBEN	REGUL	TECHN	EXP	TRUST	ATT	CO	CTRL	LIKE	PCON	PERBEN	REGUL	TECHN	EXP	TRUST										
ATT1	.92	.04	-.01	.13	-.27	.28	.22	.14	-.02	.15	.89	.28	-.02	.29	-.13	.21	.04	.15	.36	.25										
ATT2	.93	.08	.07	.09	-.32	.27	.25	.18	-.07	.23	.89	.20	.10	.15	-.27	.28	.10	.28	.22	.33										
ATT3	.89	.01	.04	.10	-.29	.29	.16	.22	-.04	.22	.89	.24	.04	.22	-.15	.31	.14	.30	.27	.28										
CO1	.04	.89	.08	-.03	.03	-.09	-.04	.11	-.01	-.10	.29	.96	.02	.22	-.10	.10	.05	.12	.21	.14										
CO2	.05	.93	.11	.04	-.02	-.05	.01	.11	.00	-.06	.18	.88	.00	.13	-.09	.04	-.03	.07	.17	.12										
CTRL1	.01	.07	.76	-.11	-.23	-.03	.19	.23	.00	.17	.01	.00	.82	-.07	-.26	.11	.22	.33	-.11	.29										
CTRL2	.07	.15	.82	-.08	-.16	.03	.08	.27	-.07	.11	.05	-.04	.85	-.07	-.21	.18	.25	.36	-.09	.22										
CTRL3	.09	.04	.87	-.16	-.22	.08	.18	.39	-.18	.22	.06	.09	.81	.00	-.22	.09	.23	.31	-.06	.19										
CTRL4	-.06	.09	.76	-.09	-.03	.11	.21	.38	-.02	.19	.02	.01	.79	.00	-.28	.05	.39	.40	-.02	.29										
LIKE1	.10	.01	-.19	.84	.06	-.01	.00	.07	.40	.09	.21	.17	-.04	.83	.03	.15	.08	.06	.42	.18										
LIKE2	.08	.00	-.01	.71	.00	.17	.19	.09	.35	.11	.20	.16	-.03	.81	.09	.06	.19	.18	.37	.09										
PCONC	-.25	-.01	-.05	.00	.75	-.14	-.21	-.24	.09	-.20	-.15	-.16	-.24	.07	.82	-.06	-.18	-.39	.12	-.36										
PCONE	-.13	.00	-.26	.09	.78	-.17	-.27	-.27	.08	-.28	-.05	-.09	-.24	.17	.76	.02	-.17	-.24	.18	-.29										
PCONSU	-.37	.01	-.12	-.02	.83	-.34	-.37	-.30	-.01	-.30	-.29	-.08	-.28	-.01	.82	-.13	-.19	-.43	.00	-.29										
PCONUA	-.25	.01	-.22	.09	.84	-.21	-.28	-.29	.09	-.32	-.13	.03	-.18	.02	.74	-.11	-.20	-.24	.06	-.29										
PERBEN1	.26	-.09	.08	.07	-.17	.84	.29	.20	.07	.26	.26	.05	.04	.18	-.04	.83	.11	.22	.00	.27										
PERBEN2	.28	-.05	.03	.10	-.28	.86	.37	.21	.05	.29	.19	.04	.08	.06	-.06	.79	.06	.08	-.05	.19										
PERBEN3	.26	-.05	.05	.05	-.26	.87	.38	.31	.07	.44	.28	.10	.19	.08	-.13	.85	.20	.28	-.03	.30										
REGUL1	.22	-.02	.17	.16	-.27	.37	.88	.29	.15	.39	.05	.01	.28	.20	-.17	.09	.85	.35	.17	.27										
REGUL2	.21	-.01	.18	.08	-.18	.42	.92	.36	.08	.40	.14	.04	.34	.07	-.28	.17	.90	.39	.09	.37										
REGUL3	.20	.00	.21	.06	-.33	.31	.91	.38	.04	.34	.07	.00	.27	.19	-.15	.14	.87	.38	.13	.30										
TECHN1	.15	.17	.38	.09	-.30	.28	.32	.91	.06	.44	.29	.13	.40	.22	-.39	.23	.39	.90	.21	.46										
TECHN2	.20	.09	.33	.11	-.34	.26	.36	.91	.10	.40	.27	.12	.40	.09	-.42	.22	.36	.91	.08	.44										
TECHN3	.18	.07	.38	.08	-.28	.22	.34	.86	.06	.40	.18	.05	.42	.08	-.33	.21	.40	.88	.10	.37										
EXP1	-.04	.02	-.07	.26	.09	.09	.07	.01	.87	-.07	.31	.17	.10	.34	.17	-.03	.14	.10	.92	-.01										
EXP2	-.04	-.03	-.09	.28	.03	.03	.09	.13	.84	.08	.29	.20	-.04	.37	.02	-.03	.12	.17	.91	.10										
TRUST1	.17	-.06	.15	.03	-.26	.29	.35	.34	-.14	.75	.22	.17	.15	.26	-.19	.21	.23	.27	.20	.67										
TRUST2	.17	-.08	.13	.21	-.24	.33	.40	.44	-.14	.83	.29	.07	.27	.11	-.35	.31	.37	.44	.05	.87										
TRUST3	.19	-.06	.24	.07	-.34	.30	.41	.42	-.01	.83	.26	.13	.28	.08	-.36	.22	.26	.46	-.06	.82										

Notes: Item codes are given in the Appendix. Privacy concerns PCON are analyzed as a second-order latent variable (see Wetzels et al. 2009) constructed by the blocks of the underlying first-order latent variables PCONC, PCONE, PCONUA, and PCONSU themselves constructed by the 15-item CFIP scale (see Appendix)

Table 2.4 Construct reliability and validity criteria, Italy and U.S.

	Italy			U.S.		
	AVE	Composite reliability	Cronbach alpha	AVE	Composite reliability	Cronbach alpha
ATT	.83	.94	.90	.79	.92	.87
CO	.83	.91	.80	.85	.92	.83
CTRL	.64	.88	.81	.67	.89	.84
LIKE	.66	.75	.34	.67	.80	
PCON	.64	.88	.82	.62	.87	.80
PERBEN	.73	.89	.82	.68	.86	.77
REGUL	.82	.93	.89	.77	.91	.85
TECHN	.80	.92	.87	.81	.93	.88
EXP	.74	.85	.64	.84	.91	.81
TRUST	.74	.84	.72	.63	.83	.71

for US and for Italy. All factor loadings (given in bold in Table 2.3) are well above the generally accepted cut-off value of .7 and exhibit generally low cross-loadings, with which individual item reliability is met. This finding suggests that the indicators accounted for a large portion of the variance of the corresponding latent constructs and therefore provided support for the convergent validity of the measures. The item reliability and internal consistency is established by the composite reliabilities of the measured constructs (Table 2.4). Compared to Cronbach's alpha (Table 2.4), which provides a lower bound estimate of the internal consistency, composite reliability is known to be a more rigorous estimate of reliability. As evident, all composite reliabilities and Cronbach alpha are high thus indicating high internal consistency. Finally, discriminant validity refers to the extent to which the measures of the different model dimensions are unique. It is generally assessed by testing whether the square root of the Average Variance Extracted (AVE) of any latent variable is greater than the correlations shared between that latent variable and other latent variables. That is, if we place the square roots of AVEs in the construct correlation matrix, the diagonal element should be greater than the off-diagonal ones for a specific construct (Table 2.5). The numbers from Table 2.5, as well as the cross-loadings in Table 2.3 clearly demonstrate adequate discriminant validity.

Structural Model

After confirming the measurement validity and reliability for both Italian and U.S. samples, we ran the structural model with all data points from both samples, consistent with the model generalizability assumption. The results of the structural model are reported in Fig. 2.2. We also provide the models for United States and Italy in Appendix 2. Since none of the tested control variables had significant effect on the attitudes, we omitted them from the figure to make it more clear and succinct.

Table 2.5 Correlation Matrix. Diagonal elements are constructs' AVEs

	Italy										U.S.									
	ATT	CO	CTRL	LIKE	PCON	PERBEN	REGUL	TECHN	EXP	TRUST	ATT	CO	CTRL	LIKE	PCON	PERBEN	REGUL	TECHN	EXP	TRUST
ATT	.83										.79									
CO	.05	.83									.27	.85								
CTRL	.04	.10	.64							.04	.01	.67								
LIKE	.12	.01	-.14	.60						.25	.20	-.04	.67							
PCON	-.32	.00	-.20	.05	.64					-.21	-.10	-.30	.07	.62						
PERBEN	.31	-.08	.07	.09	-.28	.73				.30	.09	.13	.13	-.09	.68					
REGUL	.23	-.01	.21	.11	-.36	.41	.82			.10	.02	.34	.16	-.24	.16	.77				
TECHN	.20	.12	.41	.10	-.35	.28	.38	.80		.27	.11	.55	.14	-.42	.25	.43	.81			
EXP	-.05	.00	-.09	.40	.07	.07	.10	.08	.74	.32	.21	-.08	.46	.10	-.03	.14	.14	.84		
TRUST	.22	-.08	.22	.13	-.35	.39	.50	.52	.00	.33	.14	.30	.17	-.39	.32	.36	.51	.05	.83	

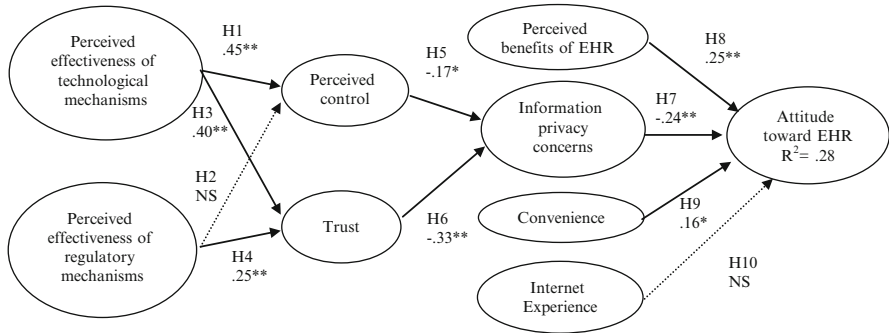


Fig. 2.2 Results of structural model testing. Notes: Path coefficients' statistical significance: *p < .05; **p < .01, NS not significant, *bold arrow* significant path; *dashed arrow* insignificant path

2.4 Discussion of Results

The results indicate overall support for our hypotheses. Eight of our ten hypotheses are supported when we test the model with the Italian and American data together. The perceived effectiveness of technology privacy mechanisms shows significant positive effect on both perceived privacy control and trust, thus supporting H1 and H3. The perceived effectiveness of privacy enhancing regulatory mechanisms, however, show positive effect only on trust (H4 supported) but not on the perceived privacy control over EHR (H2 not supported). Both trust and perceived privacy control can significantly reduce the privacy concerns towards EHR (H5 and H6 supported), and the privacy calculus components (privacy concerns, perceived benefits, and convenience) provide the significant competing influence on attitudes towards EHR (H7, H8, and H9 respectively supported). Finally, the Internet experience had no significant effect on the attitudes and thus H10 was not supported in the model testing with both nations' samples.

As we mentioned above, the structural model was run with both nations' data as one data set. Even though some national differences can be expected in the strengths of the hypothesized relationships, the general framework of the model should be valid for both nations, per the generalizability assumptions. Indeed, as discussed in the Introduction and the theoretical section, the basic arguments for the relationships in the model are not nation biased: the urgent need to implement digital health care record system; the prevalent suspicion of both American and European (Italian) citizens of possible security breaches or errors in the systems that may result in disclosure of personal health data, possibly the most sensitive type of personal data; and with this substantial loss of privacy with negative consequences for the individual. These common foundations provide the common background on which the cultural-independent view of the developed model was advanced.

In order to get deeper insight into the results of the model, and especially to interpret the lack of support for H2 and H10, we also ran two separate models with

the Italian and U.S. data. H2 remained to be insignificant for both samples. Thus, we can conclude that individuals do not tend to rely on regulatory mechanisms in building their perceived privacy control over the EHR. Only the technological privacy mechanisms enhance the perceived privacy control. A possible explanation is that individuals look at their ability to control how their health care information is collected, used, and distributed as technology empowerment rather an empowerment given by the proxy from the top. Indeed, the technological advances provide institutions with ever more sophisticated technology to empower individuals to regulate themselves how the storage and flow of their personal information is done, with which a true regulatory mechanism would not further enhance control beliefs.

We therefore find that in the technological age, users tend to look at control as a tool that they “can see and touch” and use by themselves—that is, if there is technology in place that helps them enhances their privacy, they would tend to feel more in control. The lack of support for H10 will be addressed in the limitations section.

Consistent with the trust theories (see for example (Dinev et al. 2006)) in which government regulations and institutional self-regulations play an important role in building trust, we find that, indeed, the relationship between regulatory privacy mechanisms and trust is strong and even stronger for Italy (.36 for Italy vs. .18 for US) where there is substantial more reliance on government regulations than in U.S.

Finally, it is important to note that the calculus perspective of the formation of attitudes towards EHR is evident in the model’ results. As seen from the path coefficients in Fig. 2.2, perceived benefits along with convenience *can* override the very strong impact of privacy concerns and provide an overall significant positive attitude towards EHR. Thus, the results of our model are in accordance with Angst and Agarwal (2009) who also found that “privacy concerns, while a salient barrier, may not be enough to halt the acceptance of electronic healthcare records” (p. 358) and that “through proper messaging and education, attitudes can be changes, even in the presence of great privacy concerns” (p. 360). As long as users are informed, educated, and convinced in the convenience and benefits of EHR, they would be able to form positive attitude (that would lead to adoption) even if their privacy concerns are high.

2.5 Limitations and Suggestions for Future Research

There are other model relationships that exhibit some differences between Italy and U.S. and these may be significant and due to cultural differences. While investigating the reasons and significance of these differences is beyond the limits of the current paper, they provide substantial opportunities for future research. The other insignificant relationship in the model, the impact of Internet Experience on Attitudes towards EHR (H10), demands a closer look since this is the only relationship the significance of which differs across the two nations. Indeed, the

separate model runs for both countries show a non significant relationship for Italians, but a strong (at level $p < .01$) relationship for the U.S. individuals—.35**. We believe that the explanation probably can be found with the slower rate of adoption of e-commerce in Italy in comparison to United States (Dinev et al. 2006) and the nature of the measurement that we adopted. We now realize that the measure for Internet experience (see Appendix) is biased towards Internet shopping rather than other activities. Not as many Italians shop on the Internet as Americans as evident from Table 2.2. Italians are known to actively use the Internet for social networking and communication activities rather than shopping (Dinev et al. 2006). This is a significant limitation of the study that would have not shown as such if the sample had been only American. In order to really understand how Internet and technology experience shape attitudes, further studies that lack the bias of ours are needed. We posit that the relationship will be significant for the Italians as well, thus confirming previous studies that showed positive influence of experience on attitudes.

The current study is also limited by its research question—it only looks at the individuals', citizens' calculus and cost-benefit analysis of attitudes toward EHR—and thus is a one-sided perspective. Like in every major economic development, the other side of the perspective—the institutions and their cost-benefit analysis for adoption of HER—has also to be taken into account if full understanding is sought. Recent studies have investigated this side and found that privacy protection may inhibit adoption if hospitals cannot benefit from easily exchanging patient information (Miller and Tucker 2009). According to the researchers, state privacy regulation restricting hospital release of health information reduces aggregate EMR adoption by hospitals by more than 24 % which can prevent achieving the government goal of having a national health IT network by 2014 (Miller and Tucker 2009).

2.6 Implications for Theory and Practice

Our study has several practical and theoretical implications. First, it offers a comprehensive theoretical model based on cost-benefit analysis that explains the formation of individuals' attitudes in health care context. We focused on the antecedents of information privacy concerns as well as the consequences, thus filling a gap in the privacy literature and potentially leading to a more complete understanding of this important construct. The coherently developed and rigorously tested empirical map of antecedents in this model reflects the complexity of privacy concerns formation. The study highlights the roles organizational interventions in increasing privacy control and trust, which are important in diverse sectors. These contributions lead to important implications for both practice and research.

The study's results and implications align well with the conclusion of Angst and Agarwal (2009) who found that, through message framing and persuasion, positive attitudes can be promoted even in the presence of very high privacy

concerns. Through the lens of the privacy calculus, our study shows similar path to overcoming the highly negative effect of privacy concerns in the health care and EHR context, and in addition it shows how to reduce the privacy concerns: (1) By empowering users with advanced technology to control on their own their privacy preferences, and by building trust through smart regulation and technology, we can substantially reduce privacy concerns, and (2) We can beat the negativity through convincing individuals to see the other very important components in the equation—the benefits, the convenience, the opportunity for technological advancements when implementing EHR. The results of this investigation should be of interest to government agencies which have oversight in establishing laws and regulations related to digitized health information. Individuals involved in any future efforts to evaluate the consequences of privacy policies and practices, for example, or to initiate new rulemaking procedures in this area should find this study useful. Our study shows that in order to overcome the negativity and suspicion rooted in high privacy concerns, broad and comprehensive raising of public awareness through education and communication should be implemented as to the benefits of EHR and the costs to the society and individuals if we do not implement them. The study is also very timely and relevant in the era of a concerted government and institutional effort to implement in health care comprehensive information technology solutions and digitization of records, so cost can be substantially cut and benefits to the patients enhanced.

The importance of privacy enhancing IT tools are emphasized in the recent study about the institutional EHR adoption impediments (Miller and Tucker 2009). The authors call for further research to find the optimum privacy protection that can be put in place that will minimize disruption to the diffusion and use of interdependent technologies. They refer to IT-based privacy protection (the same technological privacy control mechanisms that we are incorporating in our study) as a possible tool that can serve the balancing role and expedite adoption. We completely agree with the authors, especially in light of the recent findings by Agarwal et al. (2010) who posit that for most providers in-house development of EHR applications is neither feasible nor economical. Thus, commercial off-the-shelf solutions, especially Web-based services, will be the mainstream of digital medical records' adoption in the next few years. The adopted systems come with predefined interfaces and functionality, which may be incompatible with existing practices and the best intentions of the providers. So at this crucial moment, it is even more important for the providers to demand from the IT developers and designers a set of privacy-enhancing mechanisms and IT rules that will enable optimum control and trust by the individuals and will help advance the adoption of the digital health records.

2.7 Conclusion

Both U.S. and Europe see EHR adoption as strategic twenty-first century step to making health care more efficient, modern, with lower costs and more benefits. The research objective of this study is to investigate individuals' attitudes towards EHR

and what factors form these attitudes, themselves a strong predictor of behavior. We found that perceived effectiveness of regulatory mechanisms positively impact trust and that perceived effectiveness of technological mechanisms positively impacts perceived privacy control and trust. Both trust and perceived privacy control can substantially reduce privacy concerns which, along with perceived benefits, convenience, and Internet experience, play an important role in the privacy calculus-type formation of individual's attitudes towards EHR. Our model showed that two paths have to be undertaken by policy makers and executives to ensure wide adoption of EHR: (1) Reduce privacy concerns by enhancing trust and control beliefs (through technological and regulatory mechanisms), and (2) Overcome the negative impact of privacy concerns through raising awareness and message impact on the benefits and convenience of EHR.

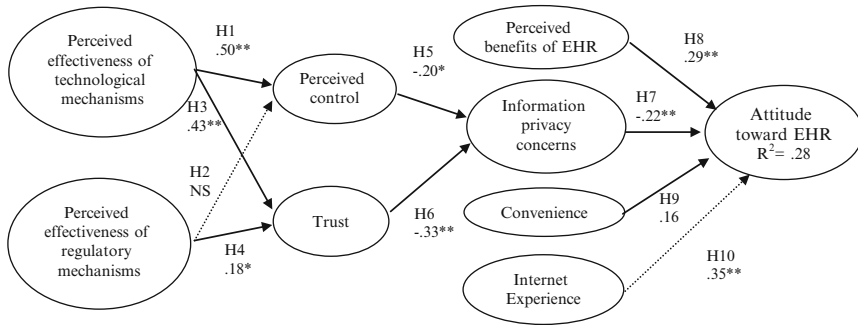
Appendix 1: Survey Instrument. All Items Were Measured on 5-Point Likert Scale, Lowest “Completely Disagree” to Highest—“Completely Agree” Unless Specified Otherwise

Construct	Code	Item (Indicate to what extent you agree with the following:)
Attitude toward EHR ATT	att1	I believe it is a good idea to have electronic health records
	att2	I believe that electronic health records is a good thing to do
	att3	I have a favorable opinion about electronic health records
Convenience CO	co1	My own online medical record would help me get all my doctors on the same page when they treat me
	co2	I'd like to have all my health information in one place—and get to it with the click of a mouse
	co3	I can access my bank account online. Why not my medical records?
	co4	I've often felt the health care system has all the power. Having my own online health record seems to even it out a little bit
	co5	I'm tired of playing 'telephone tag' with doctors and filling out the same forms. Why can't I do some of this stuff online?

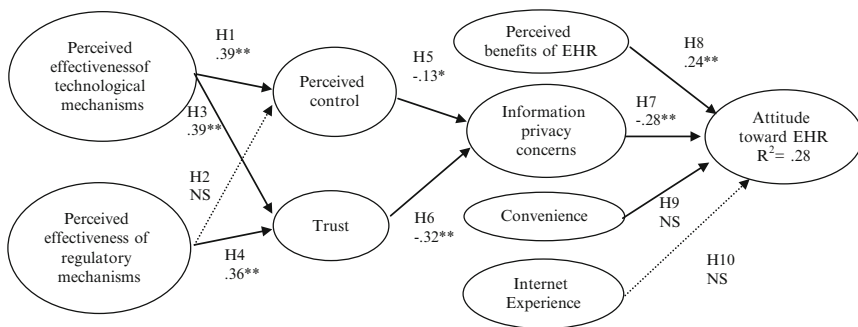
Construct	Code	Item (Indicate to what extent you agree with the following:)
		Bold items were used in the model test
Perceived privacy control CTRL	ctrl1	I think I will have control over what personal information is released by the electronic health records systems
	ctrl2	I believe I will have control over who can get access to my personal information collected by the electronic health records systems
	ctrl3	I believe I will have control over how personal information is used by the electronic health records systems
	ctrl4	In general, I believe I will be able to control my personal information provided to health care
	ctrl5	I believe I will have control over the amount of my personal information collected by the electronic health records systems
Satisfaction with current health care LIKE	like1	I like our current health care system
	like2	I believe the current health care system is good enough
Privacy concerns—collection PCONC	pconcl	It usually bothers me when health care entities ask me for personal information.
	pconcl2	When health care entities ask me for personal information, I sometimes think twice before providing it
	pconcl3	It bothers me to give personal information to so many health care entities
	pconcl4	I'm concerned that health care entities are collecting too much personal information about me
Privacy concerns—errors PCONE	pcone1	All the personal information in computer database should be double-checked for accuracy—no matter how much this costs
	pcone2	Health care entities should take more steps to make sure that the personal information in their files is accurate
	pcone3	Health care entities should have better procedures to correct errors in personal information
	pcone4	Health care entities should devote more time and effort to verifying the accuracy of the personal information in their databases
Privacy concerns—unauthorized access PCONUA	pconua1	Health care entities should devote more time and effort to preventing unauthorized access to personal information
	pconua2	Computer databases that contain personal information should be protected from unauthorized access no matter how much it costs
	pconua3	Health care entities should take more steps to make sure that unauthorized people cannot access personal information in their computers

Construct	Code	Item (Indicate to what extent you agree with the following:)
		Bold items were used in the model test
Privacy concerns—secondary use PCONSU	pconsu1	Health care entities should not use personal information for any purpose unless it has been authorized by the individuals who provided the information
	pconsu2	When people give personal information to a company for some reason, the company should never use the information for any other reason
	pconsu3	Health care entities should never sell the personal information in their computer databases to other health care entities
	pconsu4	Health care entities should never share personal information with other health care entities unless it has been authorized by the patient who provided the information
Perceived benefits PERBEN	perben1	I believe that it is beneficial for me to have my health records electronically
	perben2	I believe electronic health records will improve health care
	perben3	Electronic health records will generate positive results for the health care in our society
Perceived effectiveness of regulatory mechanisms REGUL	regul1	I believe that the law is effective in protecting me from misuse of my personal electronic health care data
	regul2	I believe that the law effectively governs the practice of how my electronic health care records are collected, used, and protected
	regul3	I believe that the current regulations are able to address violations in usage of my electronic health care records
Perceived effectiveness of technological mechanisms TECHN	techn1	I think that the electronic health records will use effective technologies
	techn2	I think that the electronic health records will use reliable technologies
	techn3	I think that there are a lot of good technologies that will help the electronic health records
Trust	trust1	I think that electronic health records are dependable
	trust2	I think that electronic health records are trustworthy
	trust3	I trust that electronic health records provide good service
Health status HS	hs	In general, would you say your health is (Poor—Excellent)
Experience with internet EXP		How frequently did you use the Internet for the following activities (Never-Always)
	exp1	Shopped or purchased something
	exp2	Made travel arrangements or bought an airline ticket
	exp3	Paid bills or managed financial accounts

Appendix 2: Structural Model for U.S. and Italy



Notes: Path coefficients' statistical significance: * $p < .05$; ** $p < .01$, NS not significant, *bold arrow* significant path, *dashed arrow* insignificant path



Notes: Path coefficients' statistical significance: * $p < .05$; ** $p < .01$, NS not significant; *bold arrow* significant path, *dashed arrow*—insignificant path

References

Agarwal R, Gao G, DesRoches C, Jha AK (2010) The digital transformation of healthcare: current status and the road ahead. *Inform Syst Res* 21(4):796–809

Ajzen I (1991) The theory of planned behavior. *Org Behav Hum Decis Process* 50(2):179–211

Ajzen I, Fishbein M (1980) *Understanding attitudes and predicting social behavior*. Prentice-Hall, Englewood Cliffs

Alonso-Zaldivar R (2009) U.S. health care lags in bang for the buck. *San Francisco Chronicle*, March 12, p. 1

- Angst MC, Agarwal R (2006a) Overcoming personal barriers to adoption when technology enables information to be available to others. In: Proceedings of 27th international conference on information systems, Milwaukee
- Angst MC, Agarwal R (2006b) Getting personal about electronic health records: modeling the beliefs of personal health record users and non-users. Working Paper, Robert H. Smith School Research Paper No. RHS-06-007. Available at SSRN: <http://ssrn.com/abstract=902904>
- Angst MC, Agarwal R (2009) Adoption of electronic health records in the presence of privacy concerns: the elaboration likelihood model and individual persuasion. *MIS Quarterly* 33(2):339–370
- Bandura A (1982) Self-efficacy mechanism in human agency. *Am Psychol* 37:122–147
- Bandura A (1986) Social foundations of thought and action. Prentice-Hall, Englewood Cliffs
- Bansal G, Zahedi F, Gefen D (2007) The impact of personal dispositions on privacy and trust in disclosing health information online. In: Proceedings of AMCIS, Paper 57. <http://aisel.aisnet.org/amcis2007/57>
- Bansal G, Zahedi FM, Gefen D (2010) The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decis Support Syst* 49:138–150
- Beatty RC, Shim JP, Jones MC (2001) Factors influencing corporate Web site adoption: a time-based assessment. *Inform Manage* 38(6):337–354
- Bishop LS, Holmes BJ, Kelley CM (2005) National Consumer Health Privacy Survey 2005. California Health Care Foundation, Oakland. <http://ehealth.chcf.org/topics/view.cfm?itemID=115694>
- Bodenheimer T, Grumbach K (2003) Electronic technology: a spark to revitalize primary care? *J Am Med Assoc* 290(2):259–264
- Cantor JD (2001) Privacy protections for cybercharts: an update on the law. *J Am Med Assoc* 285(13):1767
- Caudill ME, Murphy EP (2000) 2000 consumer online privacy: legal and ethical issues. *J Public Policy Mark* 19(1):7–19
- Chellappa RK, Sin RG (2005) Personalization versus privacy: an empirical examination of the online consumer's dilemma. *Inform Technol Manage* 6(2):181–202
- Childers TL, Carr CL, Peck J, Carson S (2001) Hedonic and utilitarian motivations for online retail shopping behavior. *J Retail* 77(4):511–535
- Choy A, Goldman J (2001) Comparing eHealth Privacy Initiatives. Health Privacy Project. Georgetown University. <http://www.chcf.org/topics/view.cfm?itemID=12739>
- Choy A, Hudson Z, Pritts J (2002) Exposed online: why the new federal health privacy regulation doesn't offer much protection to internet users, the Pew Internet and American Life Project. <http://medicalrecordrights.georgetown.edu/publications.html>
- Cimino JJ, Patel VL, Kushniruk AWT (2002) The patient clinical information system (PatCIS): technical solutions for and experience with giving patients access to their electronic medical records. *Int J Med Inform* 68(1–3):113–127
- Culnan MJ (1993) 'How did they get my name'? An exploratory investigation of consumer attitudes toward secondary information use. *MIS Quarterly* 17(3):341–364
- Culnan MJ, Armstrong PK (1999) Information privacy concerns, procedural fairness and impersonal trust: an empirical investigation. *Organ Sci* 10(1):104–115
- Culnan MJ, Bies JR (2003) Consumer privacy: balancing economic and justice considerations. *J Soc Issues* 59(2):323–342
- Dan JK, Ferrin DL, Rao HR (2008) A trust-based consumer decision-making model in electronic commerce: the role of trust, perceived risk, and their antecedents. *Decis Support Syst* 44:544–564
- Dinev T, Hart P (2004) Internet privacy concerns and their antecedents—measurement validity and a regression model. *Behav Inform Technol* 23(6):413–423
- Dinev T, Hart P (2006) An extended privacy calculus model for e-commerce transactions. *Inform Syst Res* 17(1):61–80

- Dinev T, Bellotto M, Hart P, Russo V, Serra I, Colautti C (2006) Privacy calculus model in e-commerce—a study of Italy and the United States. *Eur J Inform Syst* 15(4):389–402
- Dinev T, Hu Q, Yayla A (2008) Is there an online advertisers' dilemma? A study of click fraud in the pay-per-click model. *Int J Electron Commerce* 13(2):29–59
- Dixon P (2005) Electronic health records and the National Health Information Network: patient choice, privacy, and security in digitized environments, presented before The National Committee on Vital and Health Statistics (NCVHS) Subcommittee on privacy and confidentiality, San Francisco, CA, August 2005. <http://www.worldprivacyforum.org/pdf/pamdixonNCVHStestimonyfinal.pdf>
- Earp JB, Payton FC (2006) Information privacy in the service sector: an exploratory study of health care and banking professionals. *J Organ Comput Electron Comm* 16(2):105–122
- Faden RR, Beauchamp LT, King PMN (1986) A history and theory of informed consent. Oxford University Press, New York
- Forsythe S, Liu CL, Shannon D, Gardner LC (2006) Development of a scale to measure the perceived benefits and risks of online shopping. *J Interact Market* 20(2):55–75
- Gazzetta Ufficiale (2009) Garante per la protezione dei dati personali. Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario—16 luglio 2009. n. 178 03-08-2009. <http://www.garanteprivacy.it/garante/doc.jsp?ID=1634116>
- Gefen D, Straub DW, Boudreau MC (2000) Structural equation modeling and regression: guidelines for research practice. *Commun Assoc Inform Syst* 4(7):1–78
- Goodwin C (1991) Privacy: recognition of a consumer right. *J Public Policy Mark* 10(1):149–166
- HHS (2006) Personal health records and personal health record systems: a report and recommendations from the National Committee on Vital and Health Statistics. Department of Health and Human Services, Washington DC, February, 2006. <http://www.ncvhs.hhs.gov/0602nhiipt.pdf>
- Harris AF (2002) Interactive and Westin, The Harris Poll: #46. Harris Interactive, New York
- Hu X, Wu G, Wu Y, Zhang H (2010) The effects of Web assurance seals on consumers' initial trust in an online vendor: a functional perspective. *Decis Support Syst* 48:407–418
- Iacovou CL, Benbasat I, Dexter AS (1995) Electronic data interchange and small organizations: adoption and impact of technology. *MIS Quarterly* 19(4):465–485
- Jarvenpaa SL, Tractinsky N, Vitale M (2000) Consumer trust in an internet store. *Inform Technol Manage* 1(12):45–71
- Johnson LJ, Cullen BJ (2002) Trust in cross-cultural relationships. In: Gannon MJ, Newman KL (eds) *The Blackwell handbook of cross-cultural management*. Blackwell, Oxford, pp 335–360
- Karahanna E, Evaristo JR, Strite M (2002) Methodological issues in MIS cross cultural research. *J Global Inform Manage* 10:13–23
- Kauffman T (2006) Your health records online: OPM: benefits will outweigh risks. *Federal-Times.com*, May 15 2006. <http://federaltimes.com/index.php?S=1771146>
- Kidd MR (2008) Personal electronic health records: MySpace or HealthSpace? *Br Med J* 336:1029–1030
- Landro L (2004) Electronic medical records are taking root locally. *Wall Street J* 22:D1
- Laufer RS, Wolfe M (1977) Privacy as a concept and a social issue: a multidimensional developmental theory. *J Soc Issues* 33(3):22–42
- Liu CL (2007) Modeling consumer adoption of the internet as a shopping medium: an integrated perspective. Cambria, Youngstown
- Lo B, Clayton P, Crowley J, Glaser J, Hunter N, Koss S, Koyanagi C, Nielsen J, Shelton L, Van Amringe M (1999) Best principles for health privacy. Report for the Health Privacy Project, Georgetown University. http://www.healthprivacy.org/usr_doc/33807.pdf
- Luck J, Chang C, Brown ER, Lumpkin J (2006) Using local health information to promote public health. *Health Aff* 25(4):979–991
- Masy D, Baker D, Butros A, Cowles KE (2002) Giving patients access to their medical records via the internet: the PCASSO experience. *J Am Med Inform Assoc* 9(2):181–191
- Mayer RC, Davis JH, Schoorman FD (1995) An integrative model of organizational trust. *Academy Manage Rev* 20(3):709–734

- MacKay N, Parent M, Gemino A (2004) A model of electronic commerce adoption by small voluntary organizations. *Eur J Inform Syst* 13(2):147–159
- McKnight DH, Choudhury V, Kacmar C (2002) Developing and validating trust measures for e-commerce: an integrative typology. *Inform Syst Res* 13(3):334–359
- Miller AR, Tucker C (2009) Privacy protection and technology diffusion: the case of electronic medical records. *Manage Sci* 55(7):1077–1093
- Milne GR, Boza ME (1999) Trust and concern in consumers' perceptions of marketing information management practices. *J Interact Market* 13(1):5–24
- Milne GR, Gordon EM (1993) Direct mail privacy-efficiency trade-offs within an implied social contract framework. *J Public Policy Mark* 12(2):206–215
- Moffitt R, Manière P, Green DG, Belien P, Hjertqvist J, Breyer F (2001) Perspectives on the European health care systems: some lessons for America. Heritage Lecture #711. <http://www.heritage.org/Research/Healthcare/HL711.cfm>
- Pagliari C, Detmer D, Singleton P (2007) Potential of electronic personal health records. *Br Med J* 335:330–333
- Pavlou PA, Fygenon M (2006) Understanding and predicting electronic commerce adoption: an extension of the theory of planned behavior. *MIS Quarterly* 30(1):115–143
- Pavlou PA, Gefen D (2004) Building effective online marketplaces with institution-based trust. *Inform Syst Res* 15(1):37–59
- Phelps J, Nowak G, Ferrell E (2000) Privacy concerns and consumer willingness to provide personal information. *J Public Policy Market* 19(1):27–41
- Rindfleisch TC (1997) Privacy, information technology, and health care. *Commun ACM* 40(8):92–100
- Ringle CM, Wende S, Will S (2005) SmartPLS 2.0, Hamburg, Germany. <http://www.smartpls.de>
- Sheehan KB, Hoy GM (2000) Dimensions of privacy concern among online consumers. *J Public Policy Market* 19(1):62–73
- Skinner EA, Chapman M, Baltes PB (1988) Control, means-ends, and agency beliefs: a new conceptualization and its measurement during childhood. *J Personality Social Psychol* 54:117–133
- Shortliffe EH (1999) The evolution of electronic medical records. *Acad Med* 74(4):414–419
- Smith HJ, Milberg JS, Burke JS (1996) Information privacy: measuring individuals' concerns about organizational practices. *MIS Quarterly* 20(2):167–196
- Song J, Zahedi FM (2007) Trust in health infomediaries. *Decis Support Syst* 43:390–407
- Spiro WG, Houghteling LJ (1981) The dynamics of law, 2nd edn. Harcourt Brace Jovanovich, New York, pp 2–10
- Stewart KA, Segars AH (2002) An empirical examination of the concern for information privacy instrument. *Inform Syst Res* 13(1):36–49
- Stone EF, Gueutal GH, Gardner DG, McClure S (1983) A field experiment comparing information—privacy values, beliefs, and attitudes across several types of organizations. *J Appl Psychol* 68(3):459–468
- Stone EF, Stone DL (1990) Privacy in organizations: theoretical issues, research findings, and protection mechanisms. *Res Personnel Human Resources Manage* 8(3):349–411
- Taylor S, Todd PA (1995) Understanding information technology usage: a test of competing models. *Inform Syst Res* 6(3):144–176
- Teo TSH, Yeong YD (2003) Assessing the consumer decision process in the digital marketplace. *Omega—Int J Manage Sci* 31(5):349–363
- Tittle CR (1980) Sanctions and social deviance: the question of deterrence. Praeger, New York
- TSE (2005) Tavolo di Sanità Elettronica—Italian National Board for eHealth. A shared policy for e-Health. http://www.sanitaelettronica.gov.it/se/documenti/TSE-A_Policy_for_eHealth-ENG-DEF.pdf
- TSE (2006) Tavolo di Sanità Elettronica—Italian National Board for eHealth, Architectural Strategy for Electronic Health care. http://www.sanitaelettronica.gov.it/se/documenti/TSE_IBSE_Architectural_Strategy-ENG-DEF.pdf

- Venkatesh V, Morris MG, Davis GB, Davis FD (2003) User acceptance of information technology: toward a unified view. *MIS Quarterly* 27(3):425–478
- Westin AF (2003) Social and political dimensions of privacy. *J Soc Issues* 59(2):431
- Wetzels M, Odenkerken-Schroder G, van Oppen C (2009) Using PLS path modeling for assessing hierarchical construct models: guidelines and empirical illustration. *MIS Quarterly* 33(1):117–195
- Xin L, Li H, Zhang J, Shim JP (2010) Examining multi-dimensional trust and multi-faceted risk in initial acceptance of emerging technologies: an empirical study of mobile banking services. *Decis Support Syst* 49:222–234
- Xu H (2007) The effects of self-construal and perceived control on privacy concerns. In: *Proceedings of the 28th annual international conference on information systems (ICIS 2007)*, Montréal, Canada, Paper 125
- Xu H, Teo HH (2004) Alleviating consumer's privacy concern in location-based services: a psychological control perspective. In: *Proceedings of the twenty-fifth annual international conference on information Systems (ICIS 2004)*, Washington, DC, pp 793–806
- Xu H, Teo HH, Tan BCY (2005) Predicting the adoption of location-based services: the roles of trust and privacy risk. In: *Proceedings of 26th annual international conference on information systems (ICIS 2005)* Las Vegas, pp 897–910
- Xu H, Dinev T, Smith J, Hart P (2008) Examining the formation of individual's privacy concerns: toward an integrative view. In: *Proceedings of the international conference of information systems (ICIS 2008)*, Paris, Paper 6
- Xu H, Teo HH, Tan BCY, Agarwal R (2009) The role of Push-Pull technology in privacy calculus: the case of location-based services. *J Manage Inform Syst* 26(3):137–176
- Xu, H., Teo, H. H., Tan, B.C.Y., and Agarwal, R. (2012). Effects of Individual Self-Protection, Industry Self-Regulation, and Government Regulation on Privacy Concerns: A Study of Location-Based Services, *Information Systems Research*, 23(4): 1342–1363.
- Yamaguchi S (2001) Culture and control orientations. In: Matsumoto D (ed) *The handbook of culture and psychology*. Oxford University Press, New York, pp 223–243