DOWNLOAD PDF PRIVACY IN PERSPECTIVE

Chapter 1 : Right to privacy - Wikipedia

Enter your mobile number or email address below and we'll send you a link to download the free Kindle App. Then you can start reading Kindle books on your smartphone, tablet, or computer - no Kindle device required.

How many of you remember all the scare stories about the risks of using a credit card online from back in the mids, all of them ignoring the risks that consumers blithely took for granted in the offline world? Search engine expert Danny Sullivan vented some of this frustration on a private mailing list the other day. He gave me permission to reprint his remarks here. Danny was responding to a discussion of a Washington Post story about online privacy that started out with concerns about how information posted online is routinely being discovered and used against people in legal cases. But then, the story goes on to link these cases with the general idea of data collection online. In the 15 years since the World Wide Web brought the Internet to the masses, the most successful companies have been those that collect information about users and use it to sell things. Google, for instance, has confirmed that it keeps track of search queries sent from a particular IP address. A spokesman said the company anonymizes IP addresses associated with search queries after nine months and cookies after 18 months. Companies are loath to talk about what information they track, but internal compliance manuals for law enforcement for Facebook, Yahoo and Microsoft reviewed by The Washington Post show that their data collection is much more extensive than users might believe based on what they themselves can access. The problem with linking these two ideas is that the kind of data in the examples above is exactly the kind of data online companies need to collect in order to manage and improve their services. They are a lot like the data collected by your car â€" some of which, like your speed, is reported to you, and much of which is only reported to a mechanic via a diagnostic computer. Danny was particularly put off by the hysteria about well-known facts, and by the scrutiny given to trivial pieces of online data collection while ignoring far more massive collection of data by more familiar means. Google has confirmed it tracks queries to a particular IP address. Or as if Google ever made a secret of it. Or more to the point, like tracking to an IP address is the issue versus the bigger issue of people having search histories if people opt in linked to real, personally identifiable accounts. Seriously, sad but true I think the internet companies are indeed going to face more scrutiny, because they are big fat targets for lazy legislators who are loathe to provide some real security over, I dunno, my credit card purchases? Oh, and if you disagreed with something listed, well, good luck with getting that removed. But we tolerate that bull from our credit card companies. I have no idea at all what happens to it. They know who I called and for how long. But yeah, thank you Washington Post for focusing on the fact that Xbox Live keeps track of when I began and ended my game playing. Yeah, thanks for spending time talking about IP addresses. Could they have shoved even one paragraph of perspective in there? Could we get one of the privacy groups to maybe call for some better national standards protecting user information on and OFFline? If they are, I never hear the offline part. Years and years, rather than focusing on the bigger and more important privacy issues on a broader perspective. There are real privacy issues to be faced in the data collected by web companies. But they are part of a far bigger picture of how the world is changing. We need thoughtful understanding of what the real risks are, not finger pointing by the media and even more frighteningly, by members of Congress at companies that are easy targets because they make good political theater.

Chapter 2 : About â€“ The Privacy Perspective

This book provides a unique evolutionary perspective on the privacy debate by examining how technological advances enabled, and subsequently are eroding, a societal expectation of privacy in contemporary American society.

May, Perspective Media Ltd. The Privacy Policy describes the ways Company collects, processes and uses your Personal Information as defined below when using the Service and the rights and options available to you with respect to your information. If you have any questions about this Privacy Policy, please contact us at: What type of information do we collect? We may collect two types of information from you. The first type of information is non-identifiable information which may be made available via the use of the Site or Services. Thus, we are not aware of the identity of the user from which the Non-Personal Information was collected. The Non-Personal Information collected by us may include your aggregated usage information and technical information transmitted by your device, including but not limited to: When you access or use the Website or Service we may collect the following Personal Information: If you voluntarily subscribe to our Newsletter you will be asked to provide us with your name and email address. Any personal information or picture content that you voluntarily disclose online on discussion boards, in My Perspective feature, etc. In order to register and use the Services such as The Perspective Challenge we require basic contact information such as: Alternatively, you register to the Service via your existing third party social network account accounts such as Facebook. In the event that you register to the Services through your existing social network account, then such social network account provides us with access to certain information about you as is stored therein e. Note During the registration process you will be provided with a user name and a password, which can be replaced following login in. You represent and warrant that you are responsible for maintaining the confidentiality of your username and password and that you will not provide inaccurate, misleading or false information to us. If information provided to us subsequently becomes inaccurate, not updated, misleading or false, you will promptly notify us of such change. If we combine Personal Data with Non-Personal Data, the combined data will be treated as Personal Data for as long as it remains combined. You may upload your personal information to the Service and share the information with Company and users of the Service. The content that you upload to the Service is not private You have the control over the Content that you wish to upload to the Service. The Content you submit to the Service will be associated with your account. What does Company do with your personally identifiable information? We collect Personal Information for the following purposes: The legitimate interest of operating the service. To allow you to register for the Services To respond to claims that any content available through the Service violates rights of third-parties, to resolve disputes and enforce our policies, including investigation of potential violations thereof, for the purpose of law enforcement or in accordance with any applicable law or regulation. To post your Content on the Service and to facilitate communication between you and the Service and other users; To provide you with further marketing and advertising material, subject to your prior indication of consent on the Service. We collect Non-Personal Information for the following purposes The legitimate interest of operating the service. To perform research, analytics or for statistical purposes. To detect, prevent, or otherwise address fraud, security or technical issues. If you are under 18, please be sure to read the terms of this Privacy Policy with your parents or legal guardians. If you become aware or have any reason to believe that a Child has shared any identifiable information with us, that you want removed, please contact us at: If you are a resident of a jurisdiction where transfer of your data requires your consent, then your consent to this Privacy Policy includes your express consent for such transfer of your Personal Information. How does Company use aggregated information? Company may also use anonymous, statistical or aggregated information to properly operate the Service, to improve the quality of the Service, to enhance your experience, to create new services and features, including customized services, to change or cancel existing Content or service, for marketing and advertising purposes, and for further internal, commercial, and statistical purposes. We may share information solely in the following events: When you use the Service, or when you take part in any content-related activity. Google Analytics collects information such as how often users access the Service, what pages they visit when they do

so, etc. We use the information we get from Google Analytics only to improve our Service. Google Analytics collects certain identifiers assigned to you on the date you visit sites, rather than your name or other identifying information. We do not combine the information collected through the use of Google Analytics with personally identifiable information. You can prevent Google Analytics from recognizing you on return visits by disabling cookies on your browser. Identifiers â€" we may disclose or share identifiers collected by us as detailed above , for the purpose of operating our business and providing the Services, as well as to calculate payments and detect fraud, security or technical issues in connection with the Service; Choice.

Chapter 3 : Privacy - Wikipedia

But the right to privacy is in a general sense one of the values, and sometimes the most important value, which underlies a number of more specific causes of action, both at common law and under various statutes ".

Background[edit] State of consideration of constitutional laws and acts formed by sectors and sections Privacy uses the theory of natural rights , and generally responds to new information and communication technologies. Warren and future U. Warren and Brandeis wrote that privacy is the "right to be let alone", and focused on protecting individuals. This approach was a response to recent technological developments of the time, such as photography, and sensationalist journalism, also known as " yellow journalism ". In his widely cited dissenting opinion in Olmstead v. United States , Brandeis relied on thoughts he developed in his article The Right to Privacy. But in his dissent, he now changed the focus whereby he urged making personal privacy matters more relevant to constitutional law , going so far as saying "the government [was] identified By the time of Katz , in , telephones had become personal devices with lines not shared across homes and switching was electro-mechanical. In the s, new computing and recording technologies began to raise concerns about privacy, resulting in the Fair Information Practice Principles. Definitions[edit] In recent years there has been only few attempts to clearly and precisely define the "right to privacy". By their reasoning, existing laws relating to privacy in general should be sufficient. The right to privacy is our right to keep a domain around us, which includes all those things that are part of us, such as our body, home, property, thoughts, feelings, secrets and identity. The right to privacy gives us the ability to choose which parts in this domain can be accessed by others, and to control the extent, manner and timing of the use of those parts we choose to disclose. Westin defines privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others". Westin describes four states of privacy: These states must balance participation against norms: Each individual is continually engaged in a personal adjustment process in which he balances the desire for privacy with the desire for disclosure and communication of himself to others, in light of the environmental conditions and social norms set by the society in which he lives. David Flaherty believes networked computer databases pose threats to privacy. This concept forms the foundation for fair information practices used by governments globally. Flaherty forwards an idea of privacy as information control, "[i]ndividuals want to be left alone and to exercise some control over how information about them is used". Posner criticizes privacy for concealing information, which reduces market efficiency. For Posner, employment is selling oneself in the labour market, which he believes is like selling a product. Lessig claims "the protection of privacy would be stronger if people conceived of the right as a property right", and that "individuals should be able to control information about themselves". A collective value and a human right[edit] There have been attempts to reframe privacy as a fundamental human right , whose social value is an essential component in the functioning of democratic societies. This requires a shared moral culture for establishing social order. He claims that privacy laws only increase government surveillance. She supports a social value of privacy with three dimensions: Shared ideas about privacy allows freedom of conscience and diversity in thought. Public values guarantee democratic participation, including freedoms of speech and association, and limits government power. Collective elements describe privacy as collective good that cannot be divided. Privacy depends on norms for how information is distributed, and if this is appropriate. Violations of privacy depend on context. Shade believes that privacy must be approached from a people-centered perspective, and not through the marketplace. No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks. Privacy laws in different countries[edit] Main article: Privacy laws of the United States Although the Constitution does not explicitly include the right to privacy, the Supreme Court has found that the Constitution implicitly grants a right to privacy against governmental intrusion from the First Amendment , Third Amendment , Fourth Amendment , and the Fifth Amendment. Society of Sisters , which invalidated a successful Oregon initiative requiring compulsory public education , Griswold v. Connecticut , where a right

to privacy was first established explicitly, Roe v. Wade , which struck down a Texas abortion law and thus restricted state powers to enforce laws against abortion , and Lawrence v. Texas , which struck down a Texas sodomy law and thus eliminated state powers to enforce laws against sodomy. Strict constructionists [who? Most states of the United States[who? Intrusion upon seclusion or solitude, or into private affairs; Public disclosure of embarrassing private facts; Publicity which places a person in a false light in the public eye; and Appropriation of name or likeness. The four privacy torts above were introduced by William Prosser in his California Law Review article titled "Privacy" in However, the United States is still far behind that of European Union countries in protecting privacy online. Thus no legislation passed by the government can unduly violate it. Specifically, the court adopted the three-pronged test required for encroachment of any Article 21 right â€" legality-i. This clarification was crucial to prevent the dilution of the right in the future on the whims and fancies of the government in power. The Supreme Court must decide if the right to privacy can be enforced against private entities. Please help improve this section by adding citations to reliable sources. Unsourced material may be challenged and removed. June Learn how and when to remove this template message It is often claimed, particularly by those in the eye of the media , that their right to privacy is violated when information about their private lives is reported in the press. The point of view of the press, however, is that the general public have a right to know personal information about those with status as a public figure. This distinction is encoded in most legal traditions as an element of freedom of speech. Mass surveillance and privacy[edit] Further information: The existence of programs is justified by their conductors in terms of supposed benefits for defense and law enforcement, however this is also in conflict with the right to privacy established under various treaties, constitutions, and the Universal Declaration of Human Rights. The argument in favor of privacy has therefore come under a larger opposition to intelligence operations carried out for political purposes, and has become a contentious issue since it undermines the perceived need of nations to spy on the general population in order to maintain their power structures. Support[edit] The right to privacy is alluded to in the Fourth Amendment to the US Constitution, which states, "The right of the people to be secure in their persons, houses, papers, and effects, [a] against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. Without privacy, there would be nothing to stop a Big Brother -like entity from taking control of every aspect of life. Opposition[edit] In , during a launch event for the Jini technology, Scott McNealy , the chief executive officer of Sun Microsystems , said that privacy issues were "a red herring " and then stated "You have zero privacy anyway.

Chapter 4 : Patient Perspectives of Medical Confidentiality

By now, most people have heard of the Personal Information Protection and Electronic Documents Act (PIPEDA). Or have they? PIPEDA, or Bill C-6, first came into effect January , applying.

Margaret Mead and other anthropologists have demonstrated the ways various cultures protect privacy through concealment, seclusion or by restricting access to secret ceremonies Mead, Alan Westin has surveyed studies of animals demonstrating that a desire for privacy is not restricted to humans. However, what is termed private in these multiple contexts varies. Privacy can refer to a sphere separate from government, a domain inappropriate for governmental interference, forbidden views and knowledge, solitude, or restricted access, to list just a few. They suggested that limitations of the right could be determined by analogy with the law of slander and libel, and would not prevent publication of information about public officials running for office, for example. Warren and Brandeis thus laid the foundation for a concept of privacy that has come to be known as control over information about oneself. Although the first cases after the publication of their paper did not recognize a privacy right, soon the public and both state and federal courts were endorsing and expanding the right to privacy. In an attempt to systematize and more clearly describe and define the new right of privacy being upheld in tort law, William Prosser wrote in that what had emerged were four different interests in privacy. Public disclosure of embarrassing private facts about an individual. Publicity placing one in a false light in the public eye. Prosser noted that the intrusion in the first privacy right had expanded beyond physical intrusion, and pointed out that Warren and Brandeis had been concerned primarily with the second privacy right. Nevertheless, Prosser felt that both real abuses and public demand had led to general acceptance of these four types of privacy invasions. On his view, answers to three main questions were at the time as yet unclear: Note that Warren and Brandeis were writing their normative views about what they felt should be protected under the rubric of privacy, whereas Prosser was describing what courts had in fact protected in the 70 years following publication of the Warren and Brandeis paper. Thus it is not surprising that their descriptions of privacy differ. Thomas Nagel gives a more contemporary discussion of privacy, concealment, publicity and exposure. Despite the well-established protection of tort privacy to control information about oneself in the courts, and the almost universal acceptance of the value of informational privacy by philosophers and the populace, Abraham L. Newman and others have persuasively argued that the United States US , and multiple countries in Asia, has developed a limited system of privacy protection that focuses on self-regulation within industry and government so that personal information is often readily available. In contrast, the European Union EU and others have adopted an alternative vision highlighting consumer protection and individual privacy against the economic interests of firms and public officials. European-style privacy protection regulations have spread rapidly across the industrial world, with the United States as a major exception, and have transformed and led the global privacy debate, while the US has relied on a more laissez-faire mentality about protection of personal information and a patchwork of privacy guidelines. The European Union empowered individual privacy commissioners or group agencies that had technical expertise, were given governmental authority, and were able to form political coalitions to lobby successfully for enhanced individual privacy protection, requiring that personal information not be collected or used for purposes other than those initially intended without individual consent, and so on. This contrasts sharply with the American approach allowing entities such as insurance companies and employers ample access to personal information not covered by the separate privacy guidelines, given a lack of governmental support for more comprehensive privacy legislation and a more fragmented political system. The US has generally stood behind efficiency arguments that business and government need unfettered access to personal data to guarantee economic growth and national security, whereas the EU has sent a coherent signal that privacy has critical value in a robust information society because citizens will only participate in an online environment if they feel their privacy is guaranteed against ubiquitous business and government surveillance. It is now commonly called the constitutional right to privacy. The right was first announced in the Griswold v. The constitutional right to privacy was described by Justice William O. Douglas as protecting a zone of privacy covering the social

institution of marriage and the sexual relations of married persons. The most famous application of this right to privacy was as one justification of abortion rights defended in in Roe v. Which personal decisions have been protected by this privacy right has varied depending on the makeup of the Court. In in Bowers v. Criticism of the constitutional right to privacy has continued, particularly in the popular press, Roe v. Wade may be in jeopardy, and many viewed the Bowers decision as evidence of the demise of the constitutional right to privacy. Yet in in Lawrence v. Cohen gives a theoretical defense of this inclusive view of the constitutional right to privacy. She defends a constructivist approach to privacy rights and intimacy, arguing that privacy rights protect personal autonomy and that a constitutionally protected right to privacy is indispensable for a modern conception of reason and her interpretation of autonomy. Currently many non U. For example, constitutional privacy has been used in the U. In Europe many countries now protect same sex marriage, such as the Netherlands for over 10 years and more recently Germany since Coherentism One way of understanding the growing literature on privacy is to view it as divided into two main categories, which we may call reductionism and coherentism. Reductionists are generally critical of privacy, while coherentists defend the coherent fundamental value of privacy interests. Ferdinand Schoeman introduced somewhat different terminology which makes it easier to understand this distinction. Others have argued that when privacy claims are to be defended morally, the justifications must allude ultimately to principles which can be characterized quite independently of any concern with privacy. Consequently, the argument continues, there is nothing morally distinctive about privacy. The thrust of this complex position is that we could do quite well if we eliminated all talk of privacy and simply defended our concerns in terms of standard moral and legal categories Schoeman , 5. They deny that there is anything useful in considering privacy as a separate concept. They conclude, then, that there is nothing coherent, distinctive or illuminating about privacy interests. On the other side, more theorists have argued that there is something fundamental and distinctive and coherent about the various claims that have been called privacy interests. On this view, privacy has value as a coherent and fundamental concept, and most individuals recognize it as a useful concept as well. Those who endorse this view may be called coherentists. Nevertheless, it is important to recognize that coherentists have quite diverse, and sometimes overlapping, views on what it is that is distinctive about privacy and what links diverse privacy claims. Noting that there is little agreement on what privacy is, Thomson examines a number of cases that have been thought to be violations of the right to privacy. On closer inspection, however, Thomson believes all those cases can be adequately and equally well explained in terms of violations of property rights or rights over the person, such as a right not to be listened to. Those rights in the cluster are always overlapped by, and can be fully explained by, property rights or rights to bodily security. Privacy is derivative in its importance and justification, according to Thomson, as any privacy violation is better understood as the violation of a more basic right. Moreover, his account is unique because he argues that privacy is protected in ways that are economically inefficient. Focusing on privacy as control over information about oneself, Posner argues that concealment or selective disclosure of information is usually to mislead or manipulate others, or for private economic gain, and thus protection of individual privacy is less defensible than others have thought because it does not maximize wealth. In sum, Posner defends organizational or corporate privacy as more important than personal privacy, because the former is likely to enhance the economy. Bork views the Griswold v. Connecticut decision as an attempt by the Supreme Court to take a side on a social and cultural issue, and as an example of bad constitutional law. Douglas and his majority opinion in Griswold. Douglas had argued, however, that the right to privacy could be seen to be based on guarantees from the First, Third, Fourth, Fifth, and Ninth Amendments. Taken together, the protections afforded by these Amendments showed that a basic zone of privacy was protected for citizens, and that it covered their ability to make personal decisions about their home and family life. In contrast, Bork argues i that none of the Amendments cited covered the case before the Court, ii that the Supreme Court never articulated or clarified what the right to privacy was or how far it extended, and he charges iii that the privacy right merely protected what a majority of justices personally wanted it to cover. In sum, he accuses Douglas and the Court majority of inventing a new right, and thus overstepping their bounds as judges by making new law, not interpreting the law. Theorists including William Parent and Judith Thomson argue that the constitutional right to privacy is not really a privacy right, but is

more aptly described as a right to liberty. If so, then liberty is a broader concept than privacy and privacy issues and claims are a subset of claims to liberty. In support of this view, philosophical and legal commentators have urged that privacy protects liberty, and that privacy protection gains for us the freedom to define ourselves and our relations to others Allen, ; DeCew, ; Reiman, , ; Schoeman, , A moving account supporting this viewâ€"understanding privacy as a necessary and an indispensable condition for freedomâ€"comes from literature, here a quotation from Milan Kundera. But one day in or , with the intent to discredit Prochazka, the police began to broadcast these conversations [with Professor Vaclav Cerny, with whom he liked to drink and talk] as a radio serial. For the police it was an audacious, unprecedented act. And because the curtain-rippers were serving a hated regime, they were unanimously held to be particularly contemptible criminals. There is more detailed evidence that privacy and liberty are distinct concepts, that liberty is a broader notion, and that privacy is essential for protecting liberty. We have many forms of liberty that do not appear to have anything to do with what we might value as private and inappropriate for government intervention for personal reasons. It is clear that the U. Many tend to focus on the private as opposed to the public, rather than merely informational or constitutional privacy. If distinguishing public and private realms leaves the private domain free from any scrutiny, then these feminists such as Catharine MacKinnon are correct that privacy can be dangerous for women when it is used to cover up repression and physical harm to them by perpetuating the subjection of women in the domestic sphere and encouraging nonintervention by the state. But, Elshtain points out, this alternative seems too extreme. A more reasonable view, according to Anita Allen , is to recognize that while privacy can be a shield for abuse, it is unacceptable to reject privacy completely based on harm done in private. A total rejection of privacy makes everything public, and leaves the domestic sphere open to complete scrutiny and intrusion by the state. Yet women surely have an interest in privacy that can protect them from state imposed sterilization programs or government imposed drug tests for pregnant women mandating results sent to police, for instance, and that can provide reasonable regulations such as granting rights against marital rape. In addition, Alan Westin describes privacy as the ability to determine for ourselves when, how, and to what extent information about us is communicated to others Westin, Perhaps the best example of a contemporary defense of this view is put forth by William Parent. Parent explains that he proposes to defend a view of privacy that is consistent with ordinary language and does not overlap or confuse the basic meanings of other fundamental terms. He defines privacy as the condition of not having undocumented personal information known or possessed by others. Parent stresses that he is defining the condition of privacy, as a moral value for people who prize individuality and freedom, and not a moral or legal right to privacy. Personal information is characterized by Parent as factual otherwise it would be covered by libel, slander or defamation , and these are facts that most persons choose not to reveal about themselves, such as facts about health, salary, weight, sexual orientation, etc. Thus, once information becomes part of a public record, there is no privacy invasion in future releases of the information, even years later or to a wide audience, nor does snooping or surveillance intrude on privacy if no undocumented information is gained. In cases where no new information is acquired, Parent views the intrusion as irrelevant to privacy, and better understood as an abridgment of anonymity, trespass, or harassment. Furthermore, what has been described above as the constitutional right to privacy, is viewed by Parent as better understood as an interest in liberty, not privacy. It is too narrow an account because he only allows for a descriptive and not a normative use of the term. As another example, if personal information is part of the public record, even the most insidious snooping to attain it does not constitute a privacy invasion. Bloustein argues that there is a common thread in the diverse legal cases protecting privacy. Respect for these values is what grounds and unifies the concept of privacy. Using this analysis, Bloustein explicitly links the privacy rights in tort law described by Prosser with privacy protection under the Fourth Amendment. The common conceptual thread linking diverse privacy cases prohibiting dissemination of confidential information, eavesdropping, surveillance, and wiretapping, to name a few, is the value of protection against injury to individual freedom and human dignity. Invasion of privacy is best understood, in sum, as affront to human dignity. Although Bloustein admits the terms are somewhat vague, he defends this analysis as conceptually coherent and illuminating. On one account, privacy is valuable because intimacy would be impossible without it Fried, ;

Gerety ; Gerstein, ; Cohen, Fried, for example, defines privacy narrowly as control over information about oneself.

Chapter 5 : Perspective: Privacy policies for health social networking sites

PRIVACY IN THE WORKPLACE IN PERSPECTIVE David F. Linowes Ray C. Spencer University of Illinois This analysis examines the current state of privacy in the workplace as well as how the issue has developed over the last century.

For permission to use where not already granted under a licence please go to http: This article has been cited by other articles in PMC. Abstract Health social networking sites HSNS , virtual communities where users connect with each other around common problems and share relevant health data, have been increasingly adopted by medical professionals and patients. The growing use of HSNS like Sermo and PatientsLikeMe has prompted public concerns about the risks that such online data-sharing platforms pose to the privacy and security of personal health data. This paper articulates a set of privacy risks introduced by social networking in health care and presents a practical example that demonstrates how the risks might be intrinsic to some HSNS. The aim of this study is to identify and sketch the policy implications of using HSNS and how policy makers and stakeholders should elaborate upon them to protect the privacy of online health data. Online physician communities provide an online platform for doctors to share clinical insights, observations, and medical knowledge. Sermo is the largest physician community in which members share ideas about clinical cases, drugs, devices, and treatment options. PatientsLikeMe is a patient community that enables users to share details about their conditions, treatments, and symptoms, and provide support for one another. Although powerful, social networking also opens the door for inappropriate access, misuse, and disclosure of personal health data. Users are sharing incredible amounts of health data on diabetes-focused social networking sites, although few of these sites offer either scientific accuracy or data protection. Considering the sensitivity of health data, people may not wish for their data to be revealed to unauthorized individuals and entities because such disclosure may negatively affect reputation, 5 relationships, job opportunities, and insurance choices. There is an urgent need to address these concerns as the use of HSNS to deliver healthcare becomes increasingly common. While the privacy and security issues on HSNS are well recognized by previous research, 3 6 7 the literature specifically on the behavioral and policy issues is quite limited. This paper addresses the gap by sketching the key policy implications of using HSNS. Users are increasingly sharing their private details on such sites and, for some people, privacy takes a back seat to the hope that some exchange will help them find a better treatment, manage their condition, or improve overall health. Medical professionals also post sensitive data about their patients, community, and organizations in order to share advice on clinical situations or practice management. Second, the content produced by users may be revealed to both intended and unintended audiences. Since anybody can register on the website, anybody can view the content on the site. For example, any person or entity may create fake accounts in order to obtain data from unsuspecting users. Another related issue is that the website may exchange data with third parties without explicit consent. Some HSNS are commercial companies that have a business model based on harvesting health data for business and proprietary purposes. They may release health data to different data recipients, including doctors, pharmaceutical and medical device companies, researchers, and non-profit organizations. Aggregated health data are very valuable to commercial companies, such as drug and medical device manufacturers. Innovative data mining and health informatics technologies can link data produced from a variety of different sources to produce useful personal data aggregates or digital dossiers. Taken by themselves, certain pieces of data do not communicate much about a person, but taken together they could communicate a great deal. The digital dossiers would be immensely valuable to companies looking to market products or, in the case of insurers or employers, deny a policy or a job. The dossiers, maintained without direct government oversight, would also be an attractive target for hackers and identity thieves. Lastly, another obvious issue is the scale of the security risk. PatientsLikeMe is an online patient community that enables people with life-changing illnesses to share condition, treatment, and symptom information in order to monitor their health over time and learn from real-world outcomes. The idea was that if users could share details about their treatments, symptoms, and conditions, better treatment plans and options could be identified by the

collective wisdom on the site. As of December , there were more than registered members of PatientsLikeMe. Like most open health communities, PatientsLikeMe has an openness policy so that users can agree to share all their health data on an ongoing basis, and users from around the world have already agreed to do so. The site collects and stores two types of data from users, shared data and restricted data. Examples of shared data may include information about biography, conditions, treatments, symptoms, outcomes, laboratory results, genetic information, survey responses, and connections to other people on the site. When a user chooses to share personally identifiable information PII like their name and photograph, the information will be treated as shared data. Only when a member enters personal information such as an email address and password as part of registering to use the site, is the information treated as restricted data. According to its website, 15 every piece of information users submit to the site, except for restricted data, may be shared with the community, other users, and partners. This vulnerability is highlighted by a recent incident on the site. The user-generated content helps its partners better understand the real-world medical value of therapies, drugs, and medical devices so they can improve their products and speed up the development of new solutions for patients. Health data have also been used by its own research team to conduct studies and publish reports that are accessible to the general public. Thus, users have little control over the sharing of health data within and beyond the community. The problem is that users may skip over the terms of use and privacy policy when joining the community. Privacy policies While HSNS like PatientsLikeMe have laudable aims, including improving health outcomes and advancing medical research, the inherent openness of social networking and self-motivated data sharing, combined with extremely valuable and sensitive health data, can make users vulnerable to myriad privacy violations. The stakes increase with the amount of health data disclosed, the number of data recipients, and the increasing use and disclosure of health data for non-medical purposes. Although users may have very different viewpoints about privacy, preserving privacy can be extremely helpful for all users, and especially those with chronic diseases and those with stigmatized illnesses. The first involves the interdependencies between data sharing and risks. The amount of the data shared by users is positively correlated with their experiences of risks. The more data users share, the more risks they encounter, and the more policy attempts to limit the risks, the more it also limits the utility of the services. The only tried and true solution to social network privacy issues is either to limit the data shared or to protect the data shared. To mitigate the risks, users must share the minimum amount of personal data to accomplish the intended purpose. For instance, users may not provide PII such as their real name and national identification number. Yet, users often share many more personal details on HSNS than they would otherwise because complete information is pivotal for effective health care. Although information sharing is inextricably linked to improving health care, it is important to ensure that personal data are not inadvertently shared with an unintended audience. Some sites have multiple levels of privacy. It is critical to understand the privacy settings available within each of these sites and to apply the maximum level of privacy available. However, settings may change without prior notification, be difficult to fully implement, and ultimately will not change the content other members can access. Since users are not necessarily aware of self-protection, privacy awareness and education is an important element of the framework. Users may not wish for their personal data to be revealed to a possible unintended audience, which can include marketers, employers, insurers, and others, but they may not have the knowledge and technical skills to protect their privacy. Even in the absence of regulation, the site has an ethical duty to minimize risks to users whose data it gathers. The site should be encouraged to inform users of the dangers of inadvertently disclosing PII online. It could also provide a user-friendly way for users to protect privacy. For instance, the privacy policy could state how the individual can request removal of publicly displayed PII. Furthermore, the site could notify individuals of any material changes to its PII collection, use, or disclosure practices before making the change in the privacy policy. The third issue is how to build privacy and security into the platform while still tapping the value of user-generated content. Although some HSNS are designed in part to provide personalized health feedback to users, their business model largely depends on sharing the content with commercial entities for research and other purposes. The provider may not willingly offer too much privacy because this makes it harder for users to put their disease experiences in context and impedes the attempt to fulfill business and proprietary objectives. However, without effective privacy and

security controls, the platform can be a tempting target for malicious individuals and entities. Data anonymization techniques enable health data to be used for a wide range of purposes while minimizing the risks to individual privacy. The data exposed could be de-identified by either the safe harbor method, which requires the removal of enough PII, or the statistical method, requiring a qualified statistician to attest that the data raise very low risk of re-identification. The fourth issue is how to hold individuals and entities accountable for non-medical uses of health data. Widespread use of health data for business and proprietary purposes heightens the urgency to engage the public in a policy dialog about data privacy. The legislation should mandate that the provider must give individuals options to control how their health data are used for non-medical purposes. The legislation should further prohibit inappropriate commercial uses resulting, for example, in discrimination, even with express consent. The provider should be encouraged to enforce adequate data de-identification mechanisms against risks such as the inappropriate use and exploitation of data sharing. The legislation should also enact prohibitions for the unauthorized re-identification of anonymized data. Legislators and stakeholders could continually press the provider to adopt a privacy by regulation principle for building a privacy-sensitive site. These recommendations table 1 should inform deliberations about the privacy of online health data including HSNS and other e-health technologies. Some of the principles have been partly suggested for other online settings, including electronic medical records, 25 personal health records, 19 24 26 general social networks, 7 weblogs, 8 etc. In policy discussions we often focus on one of the three key principles and forget about the others. All three must be balanced to ensure a private and secure social network environment. Users themselves play a critical role in helping to safeguard their own data. However, users often are unaware of the risks and do not have the skills and ability to protect their privacy. The provider is reluctant to offer protections because they may reduce the benefits of open communication and data sharing. But even if privacy mechanisms were built into the platform and even if users were aware and competent in optimizing their privacy settings, users would still be exposed to potential privacy violations by the provider and its partners. Addressing these pressing challenges ultimately requires a policy framework for the access, use, and disclosure of health data for non-medical purposes. This study identified the policy implications of social networking that should inform efforts to protect the privacy of health data. Policy makers and stakeholders should elaborate upon the principles through discussions that will produce, over time, user awareness and understanding, appropriate public policies, and supportive technologies that adequately protect the privacy of online community inhabitants. Footnotes Provenance and peer review: Not commissioned; externally peer reviewed. Sharing health data for better outcomes on PatientsLikeMe. J Med Internet Res ; Quality and safety of diabetes-related online social networks. J Am Med Inform Assoc ; Toward a national framework for the secondary use of health data: The end of privacy? Blog-based applications and health information: Int J Med Inform ; Improving chronic diseases self-management through social networks.

Chapter 6 : Subscribe to read | Financial Times

The Forrester report identifies another reason that we should put privacy and security concerns in perspective: Not nearly as much data is likely to be collected or shared as some fear currently. The report notes that "privacy concerns will inhibit data economy approaches," and elaborates as follows.

Warren and Louis Brandeis wrote The Right to Privacy , an article in which they argued for the "right to be let alone", using that phrase as a definition of privacy. Nevertheless, in the era of big data , control over information is under pressure. Solitude is a physical separation from others. Physical barriers, such as walls and doors, prevent others from accessing and experiencing the individual. Richard Posner said that privacy is the right of people to "conceal information about themselves that others might use to their disadvantage". Privacy barriers, in particular, are instrumental in this process. According to Irwin Altman, such barriers "define and limit the boundaries of the self" and thus "serve to help define [the self]. Hyman Gross suggested that, without privacyâ€”solitude, anonymity, and temporary releases from social rolesâ€”individuals would be unable to freely express themselves and to engage in self-discovery and self-criticism. Personal privacy[edit] Most people have a strong sense of privacy in relation to the exposure of their body to others. This is an aspect of personal modesty. A person will go to extreme lengths to protect this personal modesty, the main way being the wearing of clothes. Other ways include erection of walls , fences , screens, use of cathedral glass , partitions, by maintaining a distance, beside other ways. People who go to those lengths expect that their privacy will be respected by others. At the same time, people are prepared to expose themselves in acts of physical intimacy , but these are confined to exposure in circumstances and of persons of their choosing. Even a discussion of those circumstances is regarded as intrusive and typically unwelcome. Fourth Amendment , which guarantees "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures". There may also be concerns about safety, if for example one is wary of becoming the victim of crime or stalking. Privacy concerns exist wherever uniquely identifiable data relating to a person or persons are collected and stored, in digital form or otherwise. In some cases these concerns refer to how data are collected, stored, and associated. In other cases the issue is who is given access to information. Various types of personal information are often associated with privacy concerns. Information plays an important role in the decision-action process, which can lead to problems in terms of privacy and availability. First, it allows people to see all the options and alternatives available. Secondly, it allows people to choose which of the options would be best for a certain situation. An information landscape consists of the information, its location in the so-called network, as well as its availability, awareness, and usability. Yet the set-up of the information landscape means that information that is available in one place may not be available somewhere else. This can lead to a privacy situation that leads to questions regarding which people have the power to access and use certain information, who should have that power, and what provisions govern it. For various reasons, individuals may object to personal information such as their religion, sexual orientation, political affiliations, or personal activities being revealed, perhaps to avoid discrimination , personal embarrassment, or damage to their professional reputations. In addition to this, financial privacy also includes privacy over the bank accounts opened by individuals. Information about the bank where the individual has an account with, and whether or not this is in a country that does not share this information with other countries can help countries in fighting tax avoidance. For example, web users may be concerned to discover that many of the web sites which they visit collect, store, and possibly share personally identifiable information about them. Similarly, Internet email users generally consider their emails to be private and hence would be concerned if their email was being accessed, read, stored or forwarded by third parties without their consent. Tools used to protect privacy on the Internet include encryption tools and anonymizing services like I2P and Tor. A right to sexual privacy enables individuals to acquire and use contraceptives without family, community or legal sanctions. Political privacy has been a concern since voting systems emerged in ancient times. The secret ballot helps to ensure that voters cannot be coerced into voting in certain ways, since they can allocate their vote as they wish in the privacy and security of the voting booth while maintaining the

anonymity of the vote. Secret ballots are nearly universal in modern democracy , and considered a basic right of citizenship , despite the difficulties that they cause for example the inability to trace votes back to the corresponding voters increases the risk of someone stuffing additional fraudulent votes into the system: Corporate privacy refers to the privacy rights of corporate actors like senior executives of large, publicly traded corporations. Desires for corporate privacy can frequently raise issues with obligations for public disclosures under securities and corporate law. Organizations may seek legal protection for their secrets. For example, a government administration may be able to invoke executive privilege [31] or declare certain information to be classified , or a corporation might attempt to protect valuable proprietary information as trade secrets. A major selling point of dial telephone service was that it was "secret", in that no operator was required to connect the call. As technology has advanced, the way in which privacy is protected and violated has changed with it. In the case of some technologies, such as the printing press or the Internet , the increased ability to share information can lead to new ways in which privacy can be breached. It is generally agreed that the first publication advocating privacy in the United States was the article by Samuel Warren and Louis Brandeis , " The Right to Privacy ", 4 Harvard Law Review , that was written largely in response to the increase in newspapers and photographs made possible by printing technologies. For example, in the United States it was thought that heat sensors intended to be used to find marijuana-growing operations would be acceptable. However, in in Kyllo v. United States U. As large-scale information systems become more common, there is so much information stored in many databases worldwide that an individual has no practical means of knowing of or controlling all of the information about themselves that others may have hold or access. The concept of information privacy has become more significant as more systems controlling more information appear. Also the consequences of privacy violations can be more severe. Privacy law in many countries has had to adapt to changes in technology in order to address these issues and, to some extent, maintain privacy rights. But the existing global privacy rights framework has also been criticized as incoherent and inefficient. Proposals such as the APEC Privacy Framework have emerged which set out to provide the first comprehensive legal framework on the issue of global data privacy. There are various theories about privacy and privacy control. The Invasion Paradigm defines privacy violation as the hostile actions of a wrongdoer who causes direct harm to an individual. This is a reactive view of privacy protection as it waits until there is a violation before acting to protect the violated individual, sometimes through criminal punishments for those who invaded the privacy of others. In the Invasion Paradigm this threat of criminal punishment that is supposed to work as deterrent. The Negative Freedom Paradigm views privacy as freedom from invasion rather than a right, going against the more popular view of a "right to privacy. Daniel Solove, a law professor at George Washington University also has a theory of privacy. He believes that a conceptualized view of privacy will not work because there is no one core element. There are many different, interconnected elements involved in privacy and privacy protection. Therefore, Solove proposes looking at these issues from the bottom up, focusing on privacy problems. People may often overlook the fact that certain elements of privacy problems are due to the structure of privacy itself. Therefore, the architecture must change wherein people must learn to view privacy as a social and legal structure. He also states that people have to redefine the relationship between privacy and businesses and the government. Participation in certain privacy elements of the government and businesses should allow people to choose whether they want to be a part of certain aspects of their work that could be considered privacy invasion. Internet privacy The Internet has brought new concerns about privacy in an age where computers can permanently store records of everything: Microsoft reports that 75 percent of U. They also report that 70 percent of U. This has created a need by many to control various online privacy settings in addition to controlling their online reputations, both of which have led to legal suits against various sites and employers. Facebook for example, as of August , was the largest social-networking site, with nearly 1, million members, who upload over 4. Twitter has more than million registered users and over 20 million are fake users. The Library of Congress recently announced that it will be acquiringâ€”and permanently storingâ€”the entire archive of public Twitter posts since , reports Rosen. According to some experts, many commonly used communication devices may be mapping every move of their users. At the heart of the Internet culture is a force that wants to find out everything about you. Actions

which take away privacy[edit] As with other concepts about privacy, there are various ways to discuss what kinds of processes or actions remove, challenge, lessen, or attack privacy. In legal scholar William Prosser created the following list of activities which can be remedied with privacy protection: Solove presented another classification of actions which are harmful to privacy, including collection of information which is already somewhat public, processing of information, sharing information, and invading personal space to get private information. Aggregating information[edit] It can happen that privacy is not harmed when information is available, but that the harm can come when that information is collected as a set then processed in a way that the collective reporting of pieces of information encroaches on privacy. Right to privacy Privacy uses the theory of natural rights, and generally responds to new information and communication technologies. In North America, Samuel D. Warren and Louis D. This citation was a response to recent technological developments, such as photography, and sensationalist journalism, also known as yellow journalism. In his widely cited dissenting opinion in Olmstead v. United States , Brandeis relied on thoughts he developed in his Harvard Law Review article in But in his dissent, he now changed the focus whereby he urged making personal privacy matters more relevant to constitutional law , going so far as saying "the government [was] identified By the time of Katz, in , telephones had become personal devices with lines not shared across homes and switching was electro-mechanical. In the s, new computing and recording technologies began to raise concerns about privacy, resulting in the Fair Information Practice Principles. Definitions[edit] In recent years there have been only few attempts to clearly and precisely define a "right to privacy. By their reasoning, existing laws relating to privacy in general should be sufficient. The right to privacy is our right to keep a domain around us, which includes all those things that are part of us, such as our body, home, property, thoughts, feelings, secrets and identity. The right to privacy gives us the ability to choose which parts in this domain can be accessed by others, and to control the extent, manner and timing of the use of those parts we choose to disclose. Westin defines privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others". Westin describes four states of privacy: These states must balance participation against norms: Each individual is continually engaged in a personal adjustment process in which he balances the desire for privacy with the desire for disclosure and communication of himself to others, in light of the environmental conditions and social norms set by the society in which he lives. David Flaherty believes networked computer databases pose threats to privacy. This concept forms the foundation for fair information practices used by governments globally.

Chapter 7 : Privacy in Perspective

privacy issues on a broader perspective. There are real privacy issues to be faced in the data collected by web companies. But they are part of a far bigger picture of how the world is changing.

Chapter 8 : The Privacy Perspective â€“ Legal blogging on the protection of privacy in the 21st century

President Trump is expected to sign into law a decision by Congress to overturn new privacy rules for Internet service providers. Passed by the Federal Communications Commission in October, the.

Chapter 9 : Privacy Policy | The Perspective

The need for a comprehensive U.S. privacy law continues to grow, but the politics, procedures and policies of privacy are too complex to move legislation through the Congress. Here's a summary of why it's so hard, followed by a new idea.