PRIVACY, INFORMATION, AND TECHNOLOGY pdf

1: Engaging Privacy and Information Technology in a Digital Age | The National Academies Press

1. Conceptions of privacy and the value of privacy. Discussions about privacy are intertwined with the use of technology. The publication that began the debate about privacy in the Western world was occasioned by the introduction of the newspaper printing press and photography.

Social Media Functions are either hosted by a third party or hosted directly on our sites. Your interactions with these features are governed by the privacy policy or statement of the company providing it. Purposes and Legal Basis for Processing Your Data We process your personal Information to operate the College and the programs you are enrolled in, to provide you with financial aid and related services such as: We also use this data to: Administer programs and course offerings, File required reports with applicable governmental authorities, Award financial aid, Administer programs and provide services, including student health and disability services, financial aid, research and reporting activities, service opportunities, and excursions for faculty led study abroad courses, Monitor trends within our student body and individual courses, Verify identity, Ensure that the College is prepared for emergencies, Enforce College policies, including but not limited to the Student Code of Conduct, and applicable laws, Manage billing, collecting, refunding and cashiering functions, Provide desktop and software support services, Deliver online courses, Coordinate events such as conferences and professional development, and Facilitate student directory and promotional activities. We combine the data that we collect in order to provide these functions. We have the following legal basis for processing the information you provide us or that we collect about you. We have a legitimate interest in retaining and educating qualified students, complying with laws and regulations that govern our conduct, and administering MMC and its programs in an efficient, ethical, and appropriate manner. We process all the information we collect from or about you to meet these purposes. Once you have accepted an offer of admission and during the period of your enrollment, we may also be required to process your Personal Information to complete a contract that you have entered into with us, including to be admitted to a program, or receive financial aid, housing, or another service from us. We may also be required to process your Personal Information to comply with laws applicable in the European Union or its member states. In the case of Sensitive Personal Information which includes information about your health, race, ethnicity, national origin, criminal convictions, religious or philosophical beliefs, sexual orientation, and trade union membership , we process information either i because we have your consent to do so or ii because we are required to process the information to comply with applicable federal and state tax, education and anti-discrimination laws. Your Personal Information is processed for purposes compatible with those already described, including for the purposes of conducting scientific, statistical, or historical research or for the purpose of creating archives in the public interest. Where possible, identifiable information is not used for these purposes, or pseudonymous data is used to limit the amount of personal Information we use in our research or archives When we process your sensitive personal information on the basis of your consent, you may withdraw that consent at any time by contacting the Executive Vice President for Administration and Finance. If you withdraw your consent, we may still be required to process your sensitive personal information to comply with applicable law, but we will explain what processing activities will continue for legal compliance purposes. MMC employees and personnel, including third parties who provide services to the College in connection with the purposes of processing described above. We share your Personal Information with our service providers only when they have agreed to process your Personal Information only to provide services to us and have agreed to protect your Personal Information from unauthorized use, access, or disclosure. Government authorities as required by laws that regulate immigration, tax, national security, and criminal activity. Data Retention We keep data about prospective student applicants for no less than 3 years, and data about actual applicants for no less than 3 years after your last semester of attendance. If you are accepted to and enroll at MMC we retain your permanent file data such as admission app and transcripts throughout your period of enrollment and for an indeterminate period thereafter. You have the right to the following information regarding processing of your Personal Information: The purposes of the processing, The categories of Personal Information concerned, The recipients or categories of recipients to whom the personal information have been or will be disclosed, Where possible, the period for which the personal information will be stored, or, if not possible, the criteria used to determine that period. You also have the following additional rights with respect to your Personal Information: The right to request access to the personal information MMC has about you, as well as the right to request rectification of any data that is inaccurate or incomplete. The right to lodge a complaint with the supervisory authority where you believe that your rights have been violated. EU residents have the right to opt out of the processing of your personal information for marketing and other purposes. EU residents have the right to erasure of your personal information when it is no longer needed for the purposes for which you provided it, as well as the right to restriction of processing of your personal information to certain limited purposes where erasure is not possible. Marymount Manhattan College Attn:

2: Information privacy - Wikipedia

Information privacy is the privacy of personal information and usually relates to personal data stored on computer systems. The need to maintain information privacy is applicable to collected personal information, such as medical records, financial data, criminal records, political records, business related information or website data.

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.

3: Information Technology: MMC Privacy Statement: Marymount Manhattan College

Information privacy, or data privacy (or data protection), is the relationship between the collection and dissemination of data, technology, the public expectation of privacy, legal and political issues surrounding them.

Internet privacy The ability to control the information one reveals about oneself over the internet, and who can access that information, has become a growing concern. These concerns include whether email can be stored or read by third parties without consent, or whether third parties can continue to track the websites that someone has visited. Another concern is if the websites that are visited can collect, store, and possibly share personally identifiable information about users. The advent of various search engines and the use of data mining created a capability for data about individuals to be collected and combined from a wide variety of sources very easily. In order not to give away too much personal information, emails should be encrypted. Browsing of web pages as well as other online activities should be done trace-less via "anonymizers", in case those are not trusted, by open-source distributed anonymizers, so called mix nets , such as I2P or Tor â€” The Onion Router. In an age where increasing amounts of information are going online, social networking sites pose additional privacy challenges. People may be tagged in photos or have valuable information exposed about themselves either by choice or unexpectedly by others. Caution should be exercised with what information is being posted, as social networks vary in what they allow users to make private and what remains publicly accessible. For example, third parties can track IP TV programs someone has watched at any given time. Medical privacy People may not wish for their medical records to be revealed to others. This may be because they have concern that it might affect their insurance coverages or employment. Or, it may be because they would not wish for others to know about any medical or psychological conditions or treatments that would bring embarrassment upon themselves. In some cases, the physician-patient privilege is legally protected. These practices are in place to protect the dignity of patients, and to ensure that patients will feel free to reveal complete and accurate information required for them to receive the correct treatment. Locational[edit] As location tracking capabilities of mobile devices are advancing location-based services , problems related to user privacy arise. Location data is among the most sensitive data currently being collected. A recent MIT study [18] [19] by de Montjoye et al. The study further shows that these constraints hold even when the resolution of the dataset is low. Therefore, even coarse or blurred datasets provide little anonymity. Political privacy Political privacy has been a concern since voting systems emerged in ancient times. The secret ballot is the simplest and most widespread measure to ensure that political views are not known to anyone other than the voters themselvesâ€”it is nearly universal in modern democracy , and considered to be a basic right of citizenship. In fact, even where other rights of privacy do not exist, this type of privacy very often does. Educational[edit] In the United Kingdom in , the Education Secretary Michael Gove described the National Pupil Database as a "rich dataset" whose value could be "maximised" by making it more openly accessible, including to private companies. An example of a data request that Gove indicated had been rejected in the past, but might be possible under an improved version of privacy regulations, was for "analysis on sexual exploitation".

4: Privacy Policy â€“ Information Technology

Healthcare Information Technology Exam Guide for CompTIA Healthcare IT Technician and HIT Pro Certifications Jan 8, by Kathleen A. McCormick R.N. and Brian Gugerty.

Conceptions of privacy and the value of privacy Discussions about privacy are intertwined with the use of technology. The publication that began the debate about privacy in the Western world was occasioned by the introduction of the newspaper printing press and photography. Since the publication of that article, the debate about privacy has been fueled by claims for the right of individuals to determine the extent to which others have access to them Westin and claims for the right of society to know about individuals. The privacy debate has co-evolved with the development of information technology. It is therefore difficult to conceive of the notions of privacy and discussions about data protection as separate from the way computers, the Internet, mobile computing and the many applications of these basic technologies have evolved. Think here, for instance, about information disclosed on Facebook or other social media. All too easily, such information might be beyond the control of the individual. Statements about privacy can be either descriptive or normative, depending on whether they are used to describe the way people define situations and conditions of privacy and the way they value them, or are used to indicate that there ought to be constraints on the use of information or information processing. Informational privacy in a normative sense refers typically to a non-absolute moral right of persons to have direct or indirect control over access to 1 information about oneself, 2 situations in which others could acquire information about oneself, and 3 technology that can be used to generate, process or disseminate information about oneself. There are basically two reactions to the flood of new technology and its impact on personal information and privacy: The other reaction is that our privacy is more important than ever and that we can and we must attempt to protect it. In the literature on privacy, there are many competing accounts of the nature and value of privacy. On one end of the spectrum, reductionist accounts argue that privacy claims are really about other values and other things that matter from a moral point of view. According to these views the value of privacy is reducible to these other values or sources of value Thomson Proposals that have been defended along these lines mention property rights, security, autonomy, intimacy or friendship, democracy, liberty, dignity, or utility and economic value. Reductionist accounts hold that the importance of privacy should be explained and its meaning clarified in terms of those other values and sources of value Westin Views that construe privacy and the personal sphere of life as a human right would be an example of this non-reductionist conception. More recently a type of privacy account has been proposed in relation to new information technology, that acknowledges that there is a cluster of related moral claims cluster accounts underlying appeals to privacy DeCew ; Solove ; van den Hoven ; Allen ; Nissenbaum , but maintains that there is no single essential core of privacy concerns. A recent final addition to the body of privacy accounts are epistemic accounts, where the notion of privacy is analyzed primarily in terms of knowledge or other epistemic states. An important aspect of this conception of having privacy is that it is seen as a relation Rubel ; Matheson ; Blaauw with three argument places: Here S is the subject who has a certain degree of privacy. Another distinction that is useful to make is the one between a European and a US American approach. A bibliometric study suggests that the two approaches are separate in the literature. In discussing the relationship of privacy matters with technology, the notion of data protection is most helpful, since it leads to a relatively clear picture of what the object of protection is and by which technical means the data can be protected. At the same time it invites answers to the question why the data ought to be protected. Informational privacy is thus recast in terms of the protection of personal data van den Hoven Examples include date of birth, sexual preference, whereabouts, religion, but also the IP address of your computer or metadata pertaining to these kinds of information. Personal data can be contrasted with data that is considered sensitive, valuable or important for other reasons, such as secret recipes, financial data, or military intelligence. Data that is used to secure other information, such as passwords, are not considered here. Although such security measures may contribute to privacy, their protection is only instrumental to the protection of other information, and the quality of such security measures is therefore out of the scope of our considerations here. A relevant distinction that has been made in philosophical semantics is that between the referential and the attributive use of descriptive labels of persons van den Hoven Personal data is defined in the law as data that can be linked with a natural person. There are two ways in which this link can be made; a referential mode and a non-referential mode. In this case, the user of the description is notâ€"and may never beâ€"acquainted with the person he is talking about or wants to refer to. If the legal definition of personal data is interpreted referentially, much of the data about persons would be unprotected; that is the processing of this data would not be constrained on moral grounds related to privacy or personal sphere of life. Personal data have become commodities. Individuals are usually not in a good position to negotiate contracts about the use of their data and do not have the means to check whether partners live up to the terms of the contract. Data protection laws, regulation and governance aim at establishing fair conditions for drafting contracts about personal data transmission and exchange and providing data subjects with checks and balances, guarantees for redress. Informational injustice and discrimination: Personal information provided in one sphere or context for example, health care may change its meaning when used in another sphere or context such as commercial transactions and may lead to discrimination and disadvantages for the individual. Encroachment on moral autonomy: Lack of privacy may expose individuals to outside forces that influence their choices. These formulations all provide good moral reasons for limiting and constraining access to personal data and providing individuals with control over their data. The basic moral principle underlying these laws is the requirement of informed consent for processing by the data subject. Furthermore, processing of personal information requires that its purpose be specified, its use be limited, individuals be notified and allowed to correct inaccuracies, and the holder of the data be accountable to oversight authorities OECD Because it is impossible to guarantee compliance of all types of data processing in all these areas and applications with these rules and laws in traditional ways, so-called privacy-enhancing technologies and identity management systems are expected to replace human oversight in many cases. The challenge with respect to privacy in the twenty-first century is to assure that technology is designed in such a way that it incorporates privacy requirements in the software, architecture, infrastructure, and work processes in a way that makes privacy violations unlikely to occur. Typically, this involves the use of computers and communication networks. The amount of information that can be stored or processed in an information system depends on the technology used. This holds for storage capacity, processing capacity, and communication bandwidth. We are now capable of storing and processing data on the exabyte level. These developments have fundamentally changed our practices of information provisioning. Even within the academic research field, current practices of writing, submitting, reviewing and publishing texts such as this one would be unthinkable without information technology support. At the same time, many parties collate information about publications, authors, etc. This enables recommendations on which papers researchers should read, but at the same time builds a detailed profile of each individual researcher. The rapid changes have increased the need for careful consideration of the desirability of effects. Some even speak of a digital revolution as a technological leap similar to the industrial revolution, or a digital revolution as a revolution in understanding human nature and the world, similar to the revolutions of Copernicus, Darwin and Freud Floridi In both the technical and the epistemic sense, emphasis has been put on connectivity and interaction. Physical space has become less important, information is ubiquitous, and social relations have adapted as well. As connectivity increases access to information, it also increases the possibility for agents to act based on the new sources of information. When these sources contain personal information, risks of harm, inequality, discrimination, and loss of autonomy easily emerge. For example, your enemies may have less difficulty finding out where you are, users may be tempted to give up privacy for perceived benefits in online environments, and employers may use online information to avoid hiring certain groups of people. Furthermore, systems rather than users may decide which information is displayed, thus confronting users only with news that matches their profiles. Although the technology operates on a device level, information technology consists of a complex system of socio-technical practices, and its context of use forms the basis for discussing its role in changing possibilities for accessing information, and thereby impacting privacy. We will discuss some specific developments and their impact in the following sections. The World Wide Web of today was not foreseen, and neither was the possibility of misuse of the Internet. Social network sites emerged for use within a community of people who knew each other in real lifeâ€”at first, mostly in academic settingsâ€”rather than being developed for a worldwide community of users Ellison It was assumed that sharing with close friends would not cause any harm, and privacy and security only appeared on the agenda when the network grew larger. This means that privacy concerns often had to be dealt with as add-ons rather than by-design. A major theme in the discussion of Internet privacy revolves around the use of cookies Palmer However, some cookies can be used to track the user across multiple web sites tracking cookies , enabling for example advertisements for a product the user has recently viewed on a totally different site. Again, it is not always clear what the generated information is used for. Laws requiring user consent for the use of cookies are not always successful, as the user may simply click away any requests for consent, merely finding them annoying. Similarly, features of social network sites embedded in other sites e. Previously, whereas information would be available from the web, user data and programs would still be stored locally, preventing program vendors from having access to the data and usage statistics. In cloud computing, both data and programs are online in the cloud , and it is not always clear what the user-generated and system-generated data are used for. Moreover, as data is located elsewhere in the world, it is not even always obvious which law is applicable, and which authorities can demand access to the data. Data gathered by online services and apps such as search engines and games are of particular concern here. Which data is used and communicated by applications browsing history, contact lists, etc. Some special features of Internet privacy social media and Big Data are discussed in the following sections. The question is not merely about the moral reasons for limiting access to information, it is also about the moral reasons for limiting the invitations to users to submit all kinds of personal information. Users are tempted to exchange their personal data for the benefits of using services, and provide both this data and their attention as payment for the services. One way of limiting the temptation of users to share is requiring default privacy settings to be strict. Also, such restrictions limit the value and usability of the social network sites themselves, and may reduce positive effects of such services. A particular example of privacy-friendly defaults is the opt-in as opposed to the opt-out approach. When the user has to take an explicit action to share data or to subscribe to a service or mailing list, the resulting effects may be more acceptable to the user. This is not only data explicitly entered by the user, but also numerous statistics on user behavior: Data mining can be employed to extract patterns from such data, which can then be used to make decisions about the user. These may only affect the online experience advertisements shown , but, depending on which parties have access to the information, they may also impact the user in completely different contexts. In particular, Big Data may be used in profiling the user Hildebrandt , creating patterns of typical combinations of user properties, which can then be used to predict interests and behavior. These derivations could then in turn lead to inequality or discrimination. When a user can be assigned to a particular group, even only probabilistically, this may influence the actions taken by others. For example, profiling could lead to refusal of insurance or a credit card, in which case profit is the main reason for discrimination. Profiling could also be used by organizations or possible future governments that have discrimination of particular groups on their political agenda, in order to find their targets and deny them access to services, or worse. Big Data does not only emerge from Internet transactions. Similarly, data may be collected when shopping, when being recorded by surveillance cameras in public or private spaces, or when using smartcard-based public transport payment systems. All these data could be used to profile citizens, and base decisions upon such profiles. For example, shopping data could be used to send information about healthy food habits to particular individuals, but again also for decisions on insurance. According to EU data protection law, permission is needed for processing personal data, and they can only be processed for the purpose for which they were obtained.

5: Privacy - Wikipedia

A thorough examination of new issues such as privacy and access to public records, government access to personal information, airline passenger screening and profiling, data mining, identity theft, consumer privacy, and financial privacy.

Electronic Privacy Information Center MIT Press, Privacy is the capacity to negotiate social relationships by controlling access to personal information. Over the last several years, the realm of technology and privacy has been transformed, creating a landscape that is both dangerous and encouraging. Significant changes include large increases in communications bandwidths; the widespread adoption of computer networking and public-key cryptography; mathematical innovations that promise a vast family of protocols for protecting identity in complex transactions; new digital media that support a wide range of social relationships; a new generation of technologically sophisticated privacy activists; a massive body of practical experience in the development and application of data-protection laws; and the rapid globalization of manufacturing, culture, and policy making. The essays in this book provide a new conceptual framework for the analysis and debate of privacy policy and for the design and development of information systems. The book provides equally strong analyses of privacy issues in the United States, Canada, and Europe. Agre, Beyond the mirror world: Privacy and the representational practices of computing Victoria Bellotti, Design for privacy in multimedia computing and communications environments Colin J. Towards a global policy for personal data protection Herbert Burkert, Privacy enhancing technologies: Typology, vision, critique Simon G. Davies, Re-engineering the privacy right: How privacy has been transformed from a right to a commodity David H. Can privacy protection be made effective? Robert Gellman, Does privacy law work? Phillips, Cryptography, secrets, and the structuring of trust Rohan Samarajiva, Interactivity as though privacy mattered Introduction words Please do not quote from this version, which changed slightly in proof. Introduction Our premise in organizing this volume is that, since the s, the policy debate around technology and privacy has been transformed. Tectonic shifts in the technical, economic, and policy domains have brought us to a new landscape that is more variegated, more dangerous, and more hopeful than before. These shifts include the emergence of digital communications networks on a global scale; emerging technologies for protecting communications and personal identity; new digital media that support a wide range of social relationships; a generation of technologically sophisticated privacy activists; a growing body of practical experience in developing and applying data protection laws; and the rapid globalization of manufacturing, culture, and the policy process. The goal of this volume is to describe this emerging landscape. By bringing together perspectives from political science, law, sociology, communications, and human-computer interaction, we hope to offer conceptual frameworks whose usefulness may outlive the frenetically changing details of particular cases. We believe that in the years ahead the public will increasingly confront important choices about law, technology, and institutional practice. This volume offers a starting point for analysis of these choices. The purpose of this introduction is to summarize and synthesize the picture of this new landscape that the contributors have drawn. First, however, I should make clear what we have not done. We have not attempted to replace the foundational analysis of privacy that has already been admirably undertaken by Allen , Schoeman , and Westin We have not replicated the fine investigative work of Burnham and Smith Nor, unlike Lyon and Zureik , have we tried to place the issues of privacy and surveillance in their broadest sociological context. Our work is organized conceptually and not by area of concern medical, financial, marketing, workplace, political repression, and so on. Although our case studies are drawn from several countries, our method is not systematically comparative see Bennett , Flaherty , and Nugter We have not attempted a complete survey of the issues that fall in the broad intersection of "technology" and "privacy. Nor, finally, do we provide a general theory of privacy or detailed policy proposals. We hope that our work will be helpful in framing the new policy debate, and we have analyzed several aspects of the development of privacy policy to date. In that period, privacy concerns focused on a small number of large centralized databases; although instrumental to the construction of the modern welfare state, these databases also recalled the role of centralized files in the fascist era. In the United States, concern about privacy arose through popular works by Ernst and Schwartz , Brenton , and Packard , as well as a detailed scholarly treatment by Westin In each case, though, the general form of the response was the same -- an enforceable code of practice that came to be known as data protection in Europe and privacy protection in the United States. The premise underlying the Code of Fair Information Practices was the same in both places: In some instances, these practices were codified by professions or industry associations. In other instances they were reduced to law. As a general matter, the focus was the centralized collection of data, specified in place and time, and under the specific responsibility of a known individual or organization. These principles and their implementation are described by Gellman. I will use the term "data protection" here. Data protection does not seek to influence the basic architecture of computer systems. Instead, it abstracts from that architecture to specify a series of policies about the creation, handling, and disposition of personal data. Mayer-Schoenberger, Bennett, and Flaherty describe the subsequent evolution of the data protection model. This model is by no means obsolete, but the world to which it originally responded has changed enormously. Some of these changes are technical. Databases of personal information have grown exponentially in number and in variety. The techniques for constructing these databases have not changed in any fundamental way, but the techniques for using them have multiplied. Data-mining algorithms, for example, can extract commercially meaningful patterns from extremely large amounts of information. Market-segmentation methods permit organizations to target their attention to precisely defined subgroups Gandy Contests, mass mailings, and other promotions are routinely organized for the sole purpose of gathering lists of individuals with defined interests. More data is gathered surreptitiously from individuals or sold by third parties. The pervasive spread of computer networking has had numerous effects. It is now easier to merge databases. As Bennett observes, personal information now routinely flows across jurisdictional boundaries. Computer networking also provides an infrastructure for a wide variety of technologies that track the movements of people and things Agre Many of these technologies depend on digital wireless communications and advanced sensors. Intelligent Transportation Systems, for example, presuppose the capacity to monitor traffic patterns across a broad geographic area Branscomb and Keller These systems also exemplify the spread of databases whose contents maintain a real-time correspondence to the real-world circumstances that they represent. These computerized mediations of personal identity have become so extensive that some authors speak of the emergence of a "digital persona" that is integral to the construction of the social individual Clarke Computer networking also provides the basis for a new generation of advanced communications media. In the context of the analog telephone system, privacy concerns e. Newer media, such as the Internet and the online services discussed by Samarajiva, capture more detailed information about their users in digital form. Digital technology also increases both the capacity of law-enforcement authorities to monitor communications and the capacity of subscribers to protect them. At the same time, the new media have provided the technical foundation for a new public sphere. Privacy activists and concerned technologists have used the Internet to organize themselves, broadcast information, and circulate software instantaneously without regard to jurisdictional boundaries. Low-cost electronic-mail alerts have been used in campaigns against consumer databases, expanded wiretapping capabilities, and government initiatives to regulate access to strong cryptography. Public-policy issues that would previously have been confined to a small community of specialists are now contested by tens of thousands of individuals. Although the success of these tactics in affecting policy decisions has not yet been evaluated, the trend toward greater public involvement has given the technology a powerful symbolic value. Potentially the most significant technical innovation, though, is a class of privacy-enhancing technologies PETs. Beginning with the publication of the first public-key cryptographic methods in the s, mathematicians have constructed a formidable array of protocols for communicating and conducting transactions while controlling access to sensitive information. These techniques have become practical enough to be used in mass-market products, and Phillips analyzes some of the sharp conflicts that have been provoked by attempts to propagate them. PETs also mark a significant philosophical shift. By applying advanced mathematics to the protection of privacy, they disrupt the conventional pessimistic association between technology and social control. No longer are privacy advocates in the position of resisting technology as such, and no longer as Burkert observes can objectives of social control if there are any be hidden beneath the mask of technical necessity. As a result, policy debates have been opened where many had assumed that none would exist, and the simple trade-off between privacy and functionality has given way to a more complex trade-off among potentially numerous combinations of architecture and policy choices. Other significant changes are political and economic. The data protection model has matured. It has become possible to ask how the effectiveness of privacy policies might be evaluated, although as both Flaherty and Bennett observe few useful methods have emerged for doing so. Pressures have arisen to tailor data protection laws to the myriad circumstances in which they are applied, with the result that sectoral regulation has spread. In the United States, as Gellman observes, the sectoral approach has been the norm by default, with little uniformity in regulatory conception or method across the various industries. In most other industrial countries, by contrast, sectoral regulation has arisen through the adaptation and tailoring of a uniform regulatory philosophy. This contrast reflects another, deeper divide. Bennett describes the powerful forces working toward a global convergence of the conceptual content and the legal instruments of privacy policy. While the United States has moved slowly to establish formal privacy mechanisms and standardize privacy practices over the last two decades, it now appears that the globalization of markets, the growing pervasiveness of the Internet, and the implementation of the Data Protection Directive will bring new pressures to bear on the American privacy regime. Mayer-Schoenberger argues that this interaction should be viewed not on a nation-by-nation basis but rather as the expression of a series of partial accommodations between the uniform regulation of data handling and liberal political values that tend to define privacy issues in terms of localized interactions among individuals. This tension runs throughout the contemporary debate and will recur in various guises throughout this introduction. One constant across this history is the notorious difficulty of defining the concept of privacy. The lack of satisfactory definitions has obstructed public debate by making it hard to support detailed policy prescriptions with logical arguments from accepted moral premises. Attempts to ground privacy rights in first principles have foundered, suggesting their inherent complexity as social goods. Bennett points out that privacy is more difficult to measure than other objects of public concern, such as environmental pollution. The extreme lack of transparency in societal transfers of personal data, moreover, gives the issue a nebulous character. Citizens may be aware that they suffer harm from the circulation of computerized information about them, but they usually cannot reconstruct the connections between cause and effect. This may account in part for the striking mismatch between public expression of concern in opinion polls and the almost complete absence of popular mobilization in support of privacy rights. One result of this unsatisfactory situation is that the debate has often returned to the basics. Mayer-Schoenberger and Davies both remark on the gap between the technical concept of data protection and the legal and moral concept of privacy, but they assign different significance to it. For Mayer-Schoenberger, the concept of data protection is well fitted to the values of the welfare state. Davies, however, focuses on the range of issues that data protection appears to leave out, and he regards the narrowly technical discourse of data protection as ill suited to the robust popular debate that the issues deserve. The basic picture, then, is as follows: Privacy issues have begun to arise in more various and more intimate ways, a greater range of design and policy options are available, and some decisions must therefore be made that are both fundamental and extraordinarily complicated.

6: Privacy and Data Security Legislation and Internet Privacy Laws

Information privacy is the right to determine when and to what extent information about oneself can be communicated to others. Information technology has created a more open society where privacy.

Privacy After you launch Lync for the first time, Lync will automatically launch every time you log in and show your presence by default. While there is no way to disable presence, you do have a few options: You can override your default presence1. You can set your preferences4 so that it does not launch upon login. Each of your contacts has one of five privacy relationships with you, and each relationship gives access to a different amount of information. By default, all contacts are the Colleagues privacy relationships. Friends and Family, as you might expect, can see more of this information than all the others. Change the privacy relationship for a contact By default, contacts are assigned the Colleagues privacy relationship when you add them to your contacts list. To view your contacts according to their privacy relationships: OpenSkype for Business, and, in your Contacts list, click the Relationships tab in the area just above your contacts other options are Groups, Status, and New. When you view your contacts by Relationships, you can drag and drop contacts into different privacy groups. To change the privacy relationship you have with a contact: In your Contacts list, right-click the contact, point to Change Privacy Relationship, and then click a new privacy relationship for the contact. Conversation history By default, instant messages and voice and video call logs are available in Lync and in an automatically generated folder in Outlook called Conversation History. To view your conversation history in Lync: Click on the messages icon in the interface. To view your conversation history in Outlook: Launch Outlook or log in at mail. Look for a folder below your inbox called Conversation History. To change the settings for saving your conversation history: If someone else has review rights for your mailbox, they will be able to see your conversation history. You can change these settings and avoid having your conversation history in Outlook by: Select Personal in the left navigation. For more information and to see examples of Level 1 confidential data, please visit http:

7: State Laws Related to Internet Privacy

Close to half the states are considering measures in to restrict how internet service providers can collect or share consumer data. This web page tracks bills that would restrict the collection or use of personal information by internet service providers (ISP). A new report identifies the.

It is approached from a socio-ethical perspective with specific emphasis on the implication for the information profession. The issues discussed are the concept privacy, he influence of technology on the processing of personal and private information, the relevance of this influence for the information profession, and proposed solutions to these ethical issues for the information profession. This is due to the development and use of technology. This paradigm shift brings new ethical and juridical problems which are mainly related to issues such as the right of access to information, the right of privacy which is threatened by the emphasis on the free flow of information, and the protection of the economic interest of the owners of intellectual property. In this paper the ethical questions related to the right to privacy of the individual which is threatened by the use of technology will be discussed. Specific attention will be given to the challenges these ethical problems pose to the information professional. A number of practical guidelines, based on ethical norms will be laid down. ETHICS The ethical actions of a person can be described in general terms as those actions which are performed within the criterium of what is regarded as good. It relates thus to the question of what is good or bad in terms of human actions. According to Spinello , p. Definition of Privacy Privacy can be defined as an individual condition of life characterized by exclusion from publicity Neetling et al. The concept follows from the right to be left alone Stair, , p. As such privacy could be regarded as a natural right which provides the foundation for the legal right. The right to privacy is therefore protected under private law. The legal right to privacy is constitutionally protected in most democratic societies. This constitutional right is expressed in a variety of legislative forms. During Australia also accepted a Privacy Charter containing 18 privacy principles which describe the right of a citizen concerning personal privacy as effected by handling of information by the state Collier, , p. Privacy is an important right because it is a necessary condition for other rights such as freedom and personal autonomy. There is thus a relationship between privacy, freedom and human dignity. In other words, it is not an absolute duty that does not allow for exceptions. Two examples can be given. A government also has the right to gather private and personal information from its citizens with the aim of ensuring order and harmony in society Ware, The right to privacy as an expression of individual freedom is thus confined by social responsibility. Different Categories of Private Information Based on the juridical definition of privacy, two important aspects which are of specific relevance for the information profession must be emphasized. The first is the fact that privacy as a concept is closely related to information - in terms of the definition of Neethling , p. Each of these categories will be briefly dealt with. This category of privacy concerns all forms of personal communication which a person wishes to keep private. The information exchanged during a reference interview between the user and the information professional can be seen as an example. This normally refers to medical information and enjoys separate legal protection Neethling, , p. According to this legislation a person has the right to be informed about the nature of an illness as well as the implications thereof. Such a person further has the right to privacy about the nature of the illness and can not be forced to make it known to others. The only exception is when the health, and possibly the lives of others may be endangered by the specific illness - such as the case may be where a person is HIV positive and the chance exists that other people may contract the virus. Personal information refers to those categories of information which refer to only that specific person, for example bibliographic name, address and financial information. This type of information is of relevance to all categories of information professionals. This information is closely related to property right. According to this a person does have control over the information which relates to personal possessions in certain instances. For example, a person may keep private the information about the place where a wallet is kept. The Expressed Will to Privacy The following important aspect of privacy is the desire for privacy by means of an expressed will since this desire is important for the delimitation of privacy. In short, the desire for privacy implies that privacy will only be at issue in cases where there is a clear expression of a desire for privacy. For example, a personal conversation between two persons will be regarded as private as long as there is an expressed will to keep it private. The moment that this will is relinquished the information is no longer regarded as private. The same applies to the other categories of personal and private information. If a person makes a private telephone number as a form of personal information known to a company, it is no longer regarded as private information. According to the law it can then even be seen as business information which may legally be traded in. This expressed will to privacy acts therefore as a very important guideline for the information professional regarding the delimitation of privacy. The confidential treatment of information is not only applicable to the above-mentioned four categories of private and personal information - it may refer to any category of information, such as, inter alia, trade secrets. Definition of Information Technology Before the influence of the use of technology in the processing of personal and private information can be dealt with, it is important to briefly pay attention to the concept technology. For the purpose of this paper the definition of Van Brakel , p. It creates the possibility of wider as well as simultaneous access to information. On the other hand, a person can be excluded from necessary information in electronic format by means of a variety of security measures such as passwords. The technological manipulation of information refers, among others, to the integration of information merging of documents , the repackaging thereof translations and the integration of textual and graphical formats and the possible altering of information changing of photographic images by electronic means. The use of technology in the processing of information can therefore not be seen as ethically neutral. By this he specifically refers to the manipulation of information by means of technology. The impact of the use of technology on the privacy of people manifests itself in a variety of areas. These areas include, inter alia the following: This relates to personal information as discussed earlier. This is done by so-called electronic eyes. The justification by companies for the use of such technology is to increase productivity. It can also lead to a feeling of fear and of all ways being watched - the so-called panopticon phenomenon. This poses an ethical problem which relates to the private communication of an individual. It is technically possible to intercept E-mail messages, and the reading thereof is normally justified by companies because they firstly see the technology infrastructure E-mail as a resource belonging to the company and not the individual, and secondly messages are intercepted to check on people to see whether they use the facility for private reasons or to do their job. By this is meant the integration of personal information from a variety of databases into one central database. The problem here does not in the first place arise from the integration of the information as such. Inside such a card a computer chip is buried that records every item purchased along with a variety of personal information of the buyer Branscomb, , p. This information obtained from the card enables marketing companies to do targeted marketing to specific individuals because the buying habits as well as other personal information of people are known. This coincides with the shift in ethical values and the emergence of the cyberpunk culture with the motto of "information wants to be free". According to an article in the IT Review , p. The Individual and Socio-economical Effect The use of technology for the processing of personal and other forms of private information has far reaching effects on society. The following effects can be distinguished: The effect on the individual can be summarized as a loss of dignity and spontaneity, as well as a threat to freedom and the right to privacy. In her research on the impact of technology on the privacy of the individual, Rosenberg , p. This brings about a redefinition of the role of society big businesses in the personal and private lives of the individual the use of personal information as a commodity. It also becomes clear that the legislation for example on E-mail on the protection of the privacy of the individual is falling behind due to the rapidly changing world of technology. Firstly, the information professional works with all four categories of personal and private information. Secondly, increasing use is made of technology in the processing thereof. Lastly, a new profession is emerging in the infopreneur whose main line of business may be the buying and selling of person-related and other private information. The Main Ethical Issues In the handling and processing of these different categories of private and personal information the information professional is confronted with the following ethical issues: This question is of utmost importance to infopreneurs. This issue refers specifically to information gained from the reference interview. According to Froehlich , Smith and Shaver et al. This issue is of specific importance in cases where an information professional is working with personal information that can have a direct influence on the life of a person. An example is the processing of medical information. The question here is whether an information professional may use any of these four categories of private information for any other reasons than the original reason given for the gathering thereof. Relating to this is the question whether the person must be notified about the way in which personal information is going to be used. This ethical problem relates to the above-mentioned questions and boils down to the question of consent of the user in terms of the use of personal information. Related questions are as follows: Applicable Ethical Norms Applicable ethical norms which can act as guidelines as well as instruments of measurement must be formulated to address these ethical issues. The following norms can be distinguished: They will be discussed briefly. Truth as an ethical norm has a dual ethical application. Firstly, it serves as norm for the factual correctness of information. As a norm it thus guides the information professional regarding the accurate and factually correct handling of private information. In the second place truth is an expression of ethical virtues such as openness, honesty and trustworthiness. According to this norm a person has the freedom to make choices in terms of freedom of privacy and freedom from intrusion. As norm, however, it may not become absolutized. Therefore the choice to privacy from intrusion may not restrict the freedom of others. This norm is closely related to freedom, but can be regarded as a more concretely applicable norm. As an individual human right it also protects the individual from unlawful interference from society amongst others the state in the private life of an individual. Ethical Guidelines for the Information Professional Based on these norms, practical guidelines for the information professional can be formulated.

8: Technology and Privacy

"The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought."â€”U.S. Supreme Court Chief Justice John Roberts in Riley v.

Information we collect When the website is accessed, the information listed below is automatically collected. Routing information â€” the Internet domain and Internet address of the computer you are using. Essential technical information â€— identification of the page or service you are requesting, type of browser and operating system you are using; and the data and time of access. Optional information â€” when you send us an email, your name, email address, and the content of your email; when you fill out online forms, all the data you choose to fill in or confirm. No other information is collected through the CPS website except when the user deliberately decides to send the information to CPS for example, by clicking on a link to send an e-mail. Cookies may be implemented on cpschools. Google Analytics Google Analytics is a web-based tool that collects information such as web browser used, date, time and frequency of pages visited on all cpschools. Chesapeake Public Schools uses information from Google Analytics to improve the quality of cpschools. Google Analytics may collect specific information you have shared with google including but not limited to the IP address assigned to your computer on the date you visit. Although Google Analytics uses cookies to identify you as a unique user and details about your visit to cpschools. You can prevent Google Analytics from recognizing you on return visits to this site by disabling cookies in your browser. CPS may keep user information indefinitely, but ordinarily the routing information is deleted on a routine basis. No attempt is made to link routing information to the individuals browsing the CPS website. CPS may also use routing information in a statistical summary-type format to assess site content and server performance. CPS may share this summary information with business partners when needed. Essential and nonessential technical information helps CPS respond to user request in an appropriate format or in a personalized manner and helps CPS to plan website improvements. Optional information is retained in accordance with the records retention schedules at the Library of Virginia. Under FOIA, any records in the possession of CPS at the time of Freedom Of Information Request may be subject to being inspected by or disclosed to members of the public for any purpose they may desire. Choice to provide information There is no legal requirement for a website user to provide any information at the CPS website. However, the CPS website cannot be accessed without routing information and the essential technical information. Failure to provide optional information may mean that the particular feature or service associated with that part of the web page would not be available to the user. Customer comments or review Questions about this privacy statement or the practices of the CPS website or requests to review or correct any information collected by the website should be directed to the Department of Information Technology, Chesapeake Public Schools, Adopted March 22,

9: Privacy and Information Technology (Stanford Encyclopedia of Philosophy)

A, Appendix III, Management of Federal Information Resources, which establishes guidelines for Federal agencies on complying with the fair information practices and security requirements for operating automated information systems; and.

PRIVACY, INFORMATION, AND TECHNOLOGY pdf

Beginning theory by peter barry Meat and Beans (Blastoff! Readers (The New Food Guide Pyramid (The New Food Guide Pyramid) Political reconstruction in Germany, zonal and interzonal, by Karl Loewenstein. Electronic Devices and Circuit Theory (9th Edition) Zoom mrs 802 manual Everyday use by alice walker analysis ARM system architecture History of Milan under the Sforza Gay marriage and democracy Algorithms and Parallel Vlsi Architectures/Vols. A and B The New Experimental Design Lonely Planet Thailand, Vietnam, Laos Cambodia Road Atlas (Travel Atlases) VLF mapping of geological structure International Justice in Rwanda and the Balkans Those Can-Do Pigs Promises to make a gift Illustrations in childrens books. Wondershare editor registration code Walworth co phone book The earth as modified by human action You never get a second chance to make a first impression : behavioral consequences of first impressions Racial mental differences. V. 1 Parts 1 to 3. 1907. Business book summary filetype Cash for the Final Days Abstracts of the Collected works of C.G. Jung Environment and energy: Environmental aspects of energy production and use with particular reference to n An ordinance of Parliament Modern Islamic art Pennsylvanias Delaware Division Canal Ben Jonson Plays Complete Collection Vol I Christian Education for My First Grader Is he a lying, cheating sunofabitch? More! Low Carb Recipes Fast Easy The congresswomen (Ecclesiazusae). 1.1.3 Ethiopic Enoch Green fingers, by A. C. Clarke. Baptized green Art Goodtimes All Change and Other Plays (Playscripts) The Black family in slavery and freedom, 1750-1925