DOWNLOAD PDF TECHNOLOGY AND PRIVACY

Chapter 1 : The Real Privacy Problem - MIT Technology Review

"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.

How to Protect Your Online Privacy: A Practical Guide November 7, Do you take your online privacy seriously? They have an ideal scenario of just how private their online activities should be, but they rarely do anything to actually achieve it. All You Need to Know November 6, We rely on our phones to process and store reams of personal digital data. Our digital activities -- from checking bank balances to paying for a product with a tap of the screen, to sending friends and family messages over social media, to accessing work emails remotely -- have turned our phones into a goldmine of personal information. How secure is your mobile device? She is an authority on Internet security, data breaches and fraud mitigation. Bush and his staff. In the shadow of Brexit, it apparently has decided it has the real enemy of the people in its sights: Given that it actually does fall within the legitimate purview of government, it is hard not to agree. Forty-two percent of the roughly 4, people who responded to the May poll said they had taken a break of several weeks from checking the platform. Cortana will be available on amazon Echo devices, while Alexa will be available on Windows 10 devices and on Harman Kardon Invoke speakers. The issue came to a head in part due to recent breaches that exposed the personal data of millions of American consumers. However, the CCPA also addresses other privacy incidents. Earrings With Earphones and a Smartphone Bonanza July 26, Swings Bluetooth Earrings with built-in earphones showcase a practical, clever idea for people with pierced ears. You can expect five hours of listening time out of the Swings on a single charge. However, the protection may be weak at best. In some cases, the phone might not charge, according to Apple. The fitness app, Polar Flow, publicized more data about its users in a more accessible way than comparable apps, investigators found. The practices nudged users toward accepting privacy options that favored the tech companies rather than themselves, the NCC found. Facebook and Google have no intention of providing users with an actual choice, the NCC has claimed. The company included this feature in the developer versions of iOS Cloud Health Services, Part 2: Privacy and Security May 23, Health services vendors have been partnering with various organizations to gain a foothold in the cloud and to test out their solutions. This success comes at a time when kids appear to be increasingly at risk from rogue school shooters and the United States government seems deadlocked on gun control. Providers have strongly objected to releasing customer information residing outside the U. The providers noted a potential "staggering" loss of international customers. Russia used social media as a big part of that effort. By injecting malicious snippets of text into encrypted messages, attackers can use the flaw to make the email client exfiltrate decrypted copies of the emails, explained the authors, a team of researchers from three European universities. May 3, Facebook plans to offer members a tool that to prevent tracking of their online activity outside the network. The Clear History feature will allow users to see which websites and applications send Facebook information when they use them, delete the data and prevent Facebook from collecting and storing it in the future. It will take a few months to build the tool, Facebook said. Fitbit also will move to the Google Cloud Platform to innovate and advance its products and services. Could BlackBerry Displace Apple? April 30, I spent a day with BlackBerry last week and it brought back memories of how Apple displaced the company around a decade ago. I, like a lot of folks, thought what Apple was attempting was impossible. BlackBerry largely has completed its pivot to software and services, but a wave of new phones from its partners suggests new possibilities. Gmail Privacy and Security Get Ruggedized April 26, Google has rolled out a number of new features designed to make its G Suite collaboration and productivity apps more efficient and safer to use. G Suite currently has more than 4 million paying business customers. The updates include a new design, enhanced security and AI components, and better integration of G Suite apps -- including Gmail, which is getting a brand new look. The robot could be a mobile smart speaker. Some versions of the product apparently have cameras and computer vision software. However, I think this is only a step in the path that governments -- and I do mean more than the U.

Chapter 2 : Technology Impact on Privacy

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.

Kafka , The Penal Colony The industrial age was dependent on technologies that extracted value from the earth, trees, and water. Our age too relies on extractive technologies. However the technologies are not pumps or drills, nor is the substance extracted valued because of its physical properties. The technologies are computers, transmitters, spectrographs and video lens. A major substance extracted is personal information. In United States Supreme Court Justice Brandeis wrote "discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack to obtain disclosure in court of what is whispered in the closet. The progress of science in furnishing the government with means of espionage is not likely to stop with wiretapping. New technologies for collecting personal information which transcend the physical, liberty enhancing limitations of the old means are constantly appearing. They probe more deeply, widely and softly than traditional methods, transcending barriers whether walls, distance, darkness, skin or time that historically protected personal information. The boundaries which have defined and given integrity to social systems, groups and the self are increasingly permeable absent special precautions. The power of governmental and private organizations to compel disclosure whether based on technology, law or circumstance and to aggregate, analyze and distribute personal information is growing rapidly. We are becoming a transparent society of record such that documentation of our past history, current identity, location, communication and physiological and psychological states and behavior is increasingly possible. With predictive profiles and DNA there are even claims to be able to know individual futures. Information collection often occurs invisibly, automatically and remote --being built into routine activities. Awareness and genuine consent on the part of the subject may be lacking. The amount of personal information collected is increasing. New technologies have the potential to reveal the unseen, unknown, forgotten or withheld. People are in a sense turned inside out. To be alive and a social being is to automatically give off signals of constant information--whether in the form of heat, pressure, motion, brain waves, perspiration, cells, sound, olifacteurs, waste matter, or garbage, as well as more familiar forms such as communication and visible behavior. These remnants are given new meaning by contemporary surveillance technologies. Through a value-added, mosaic process, machines often with only a little help from their friends may find significance in surfacing and combining heretofore meaningless data. The ratio of what individuals know about themselves or are capable of knowing vs. Data in diverse forms from widely separated geographical areas, organizations and time periods can be easily merged and analyzed. In relatively unrestrained fashion new and old organizations are capturing, combining and selling this information, or putting it to novel internal uses. In the United States we celebrated the th anniversary of the Constitution , a document that extended liberty. Bentham offered a plan for the perfect prison in which there was to be constant inspection of both prisoners and keepers. His ideas helped give rise to the maximum security prison. The stark situation of the maximum security prison can help us understand societal developments. Many of the kinds of controls and information gathering techniques found in prison and in the criminal justice system more broadly, are diffusing into the broader society. We may become a "maximum security society. Information leakage is rampant. Indeed it is hemorrhaging, as traditional boundaries disappear. The line between the public and the private is weakened; we are under increased observation, ever more goes on a permanent record, and much of what we say, do and even feel may be known and recorded by others we do not kno-- whether we will this or not, and even whether we know about it or not. Data in many different forms, from widely separated geographical areas, organizations, and time periods can easily be merged and analyzed. As the technology becomes ever more penetrating and intrusive, it becomes possible to gather information with laser-like specificity and with sponge-like absorbency. If we think about the information gathering net as being parallel to a fishing net, then the mesh of the net has become finer and the net wider. It is easy to get carried away with science fiction fantasies about

things that might happen. But looking just to the next decade we will likely see technical developments with implications for personal privacy such as the following: DNA screening and monitoring. It is increasingly easy to know "more" about others without their knowledge or consent. Technology creates new possibilities for the invasion of privacy and other problems which our laws, policy, manners and culture have not kept pace with. The increased availability of personal information whether in audio, visual, telemetric , bio-chemical, or data base forms is a tiny strand in the constant expansion of knowledge witnessed in the last two centuries and of the centrality of information to the working of contemporary society. As a sociologist, my research interest is in the new technologies and questions and themes these raise about the individual and society. Under what conditions is it appropriate to gather personal information and what are the social correlates and consequences of revealing or concealing it? A morality for the collection of personal data ought not to depend on how weak or powerful a means is, but on more transcendent ideas about what is right and wrong and the social consequences. The new information technologies involve larger issues regarding the complex inter-relations of technology and society; the growth of large governmental and private organizations; information flows and restrictions in a democratic society; the social functions and dysfunctions of anonymity; the public and the private; and the nature and experiencing of trust and distrust, the social bond, and social control in mass society. To the extent that the vast increase in what can be known about the individual is joined with a declining ability to protect that information, the implications are profound for behavior and social organization. Most analyses focus on only one technology such as telecommunications, computer data bases, drug testing or location monitoring or apply only one perspective-- technical, ethical, legal, social or policy. In a forthcoming book tentatively called Windows into the Soul: Surveillance and Society in An Age of High Technology I seek to be integrative and comprehensive-- looking across technologies, disciplines and methods. I treat the various extractive technologies as a unit and from a variety of perspectives. I suggest cross-cutting analytic dimensions which permit uniting seemingly dissimilar, and separating seemingly similar, phenomena. I offer a set of questions and concepts intended to help in understanding and contrasting extractive technologies, regardless of their specifics. In a previous study of undercover police practices I focused on human informers and infiltrators as the means of data collection, while for this project material technologies are central. The new information technologies raise at least four broad types of question: What theories or ideas best account for the observed patterns and trends? Why have we seen such a rapid expansion in the diffusion of these technologies in the last decade? What inhibits or facilitates the use of extractive technologies? What social processes of facilitation and resistance can be identified? What are the implications for the changing nature of, and the social functions and dysfunctions of borders and boundaries? What type of society would we have if there was greatly enhanced visibility for our current actions and thoughts, as well as for the past and the future? Secondly, the techniques occur within and against a cultural backdrop and personal experience which must be understood. How are these techniques treated in popular culture as represented by advertisements, cartoons, jokes, music, art and surveillance toys for children? What images and symbols predominate? What does this material tell us about the lived experience of being either the watcher or the watched? This material raises major questions for our comparative understanding of different societies. This is particularly important in an age of globalization where communications technologies weaken borders. Societies and regional complexes such as Northern vs. Southern Europe or Europe vs. North America, Asia vs. An issue of particular importance is that of public policy and ethics. How should the technologies be judged? What is at stake? What competing values are present and how can and have conflicts between them been responded to? What is most problematic or desirable about extractive technologies? What are the major forms of abuse and how can they be minimized? What are the social consequences of control as a result of etiquette, organizational policies, laws and the design of technology? The first part of the Appendix suggests a number of general questions that can be asked of any new technology. The second part deals with information technologies and, by way of illustration with the information highway specifically. The specific questions offered here can guide research and policy. In the remainder of this paper I wish to do three things 1 discuss the issue of privacy and why it is important 2 list some techno-fallacies regarding information technology and 3 list some principles that can guide us in the development and use of new these technologies. The new

technologies may raise a variety of troubling issues including injustice, intrusion, denial of due process, absence of informed consent, deception, manipulation, errors, harassment, misuse of property and lessened autonomy. Privacy as it involves the control of personal information is central to many of the social concerns raised by new information technologies. The United States does not have the recent European experience with totalitarian governments , and has a rather uncritical view of technology. Those factors, when joined with the value placed on free enterprise, rampant consumerism, freedom of speech and information, and concerns over declining productivity in a global economy, AIDS , drug use and crime mean that in the United States the laws and policies for the protection of personal information are much weaker than in Europe. For example there are no data protection commissions or commissioners. Personal information is commodified e. One response to privacy concerns often expressed by some industry spokespersons and many citizens is simply, "So what? We increasingly live in a world of strangers, rather than in homogeneous rural communities in which people knew those with whom they had contact. The United States Supreme Court has said in its famous Katz decision that privacy was only protected when it could be reasonably expected. With more powerful technologies we can reasonably expect less and less and hence privacy must become more restricted. Most so-called "privacy invasions" are not illegal in the United States. Given the free market, you can also buy technologies to protect yourself from privacy invasion. Personal information is often viewed as just another commodity to be sold like any other. Companies have an obligation to stockholders to make money. Government must find the guilty and protect the innocent. In addition we are an open society that believes that visibility in government brings accountability. With respect to individuals a valued legacy of the s is personal openness and honesty. The only people who worry about privacy are those who have something to hide.

Chapter 3 : Privacy Lost: Does anybody care? - Technology & science - Privacy Lost | NBC News

Technology, broadly, which includes the fields of marketing and information technology, has taken a big hit financially following the revelation of the NSA's surveillance program and the government's eavesdropping on tech companies.

Instead, we need a civic solution, because democracy is at risk. In , The Public Interest, then a leading venue for highbrow policy debate, published a provocative essay by Paul Baran, one of the fathers of the data transmission method known as packet switching. We could check to see whether the local department store has the advertised sports shirt in stock in the desired color and size. We could ask when delivery would be guaranteed, if we ordered. The information would be up-to-the-minute and accurate. We could pay our bills and compute our taxes via the console. We would obtain up-to-the-minute listing of all television and radio programs â€¦ The computer could, itself, send a message to remind us of an impending anniversary and save us from the disastrous consequences of forgetfulness. But he was prescient enough to worry that utility computing would need its own regulatory model. Here was an employee of the RAND Corporationâ€”hardly a redoubt of Marxist thoughtâ€”fretting about the concentration of market power in the hands of large computer utilities and demanding state intervention. Because of the difficulty in rebuilding complex systems to incorporate safeguards at a later date, it appears desirable to anticipate these problems. All the privacy solutions you hear about are on the wrong track. The problem was recognized early on, and little was done about it. Ordering shirts, paying bills, looking for entertainment, conquering forgetfulness: By the s, however, many digital enthusiasts believed otherwise; they were convinced that the spread of digital networks and the rapid decline in communication costs represented a genuinely new stage in human development. If only we could now erase the decade we lost and return to the utopia of the s and s by passing stricter laws, giving users more control, and building better encryption tools! A different reading of recent history would yield a different agenda for the future. The widespread feeling of emancipation through information that many people still attribute to the s was probably just a prolonged hallucination. Both capitalism and bureaucratic administration easily accommodated themselves to the new digital regime; both thrive on information flows, the more automated the better. Something else is needed: Even programs that seem innocuous can undermine democracy. Yes, the commercial interests of technology companies and the policy interests of government agencies have converged: Google and Facebook are compelled to collect ever more data to boost the effectiveness of the ads they sell. Many of those programs deal with national security. But such data can be used in many other ways that also undermine privacy. The Italian government, for example, is using a tool called the redditometro, or income meter, which analyzes receipts and spending patterns to flag people who spend more than they claim in income as potential tax cheaters. Once mobile payments replace a large percentage of cash transactionsâ€”with Google and Facebook as intermediariesâ€”the data collected by these companies will be indispensable to tax collectors. Likewise, legal academics are busy exploring how data mining can be used to craft contracts or wills tailored to the personalities, characteristics, and past behavior of individual citizens, boosting efficiency and reducing malpractice. A new book by three British academicsâ€” Changing Behaviours: On the Rise of the Psychological State â€”features a long list of such schemes at work in the U. Thanks to smartphones or Google Glass, we can now be pinged whenever we are about to do something stupid, unhealthy, or unsound. Citizens take on the role of information machines that feed the techno-bureaucratic complex with our data. Even if we tie the hands of the NSAâ€”by some combination of better oversight, stricter rules on data access, or stronger and friendlier encryption technologiesâ€”the data hunger of other state institutions would remain. They will justify it. On issues like obesity or climate changeâ€”where the policy makers are quick to add that we are facing a ticking-bomb scenarioâ€”they will say a little deficit of democracy can go a long way. It replaces the messy stuff of coalition-building, bargaining, and deliberation with the cleanliness and efficiency of data-powered administration. This phenomenon has a meme-friendly name: In essence, information-rich democracies have reached a point where they want to try to solve public problems without having to explain or justify themselves to citizens. Instead, they can simply appeal to our own self-interestâ€”and they know enough about us to engineer a perfect, highly

personalized, irresistible nudge. Privacy is a means to democracy, not an end in itself. Another warning from the past. His lecture explored the very same issue that preoccupied Baran: He also recognized that privacy is not an end in itself. Insurance companies could tailor cost-saving programs to the needs and demands of patients, hospitals, and the pharmaceutical industry. Welfare agencies could suddenly unearth fraudulent behavior. But how would these technologies affect us as citizensâ€"as subjects who participate in understanding and reforming the world around us, not just as consumers or customers who merely benefit from it? In case after case, Simitis argued, we stood to lose. Instead of getting more context for decisions, we would get less; instead of seeing the logic driving our bureaucratic systems and making that logic more accurate and less Kafkaesque, we would get more confusion because decision making was becoming automated and no one knew how exactly the algorithms worked. We would perceive a murkier picture of what makes our social institutions work; despite the promise of greater personalization and empowerment, the interactive systems would provide only an illusion of more participation. Zarsky sees vast implications for democracy here: A non-interpretable process might follow from a data-mining analysis which is not explainable in human language. Here, the software makes its selection decisions based upon multiple variables even thousands â€¦ It would be difficult for the government to provide a detailed response when asked why an individual was singled out to receive differentiated treatment by an automated recommendation system. The most the government could say is that this is what the algorithm found based on previous cases. This is the future we are sleepwalking into. Too little privacy can endanger democracy. But so can too much privacy. Simitis got the trends right. Traditionally, our response to changes in automated information processing has been to view them as a personal problem for the affected individuals. But this right, disconnected from any matching responsibilities, could also sanction an excessive level of withdrawal that shields us from the outside world and undermines the foundations of the very democratic regime that made the right possible. This is not a problem specific to the right to privacy. For some contemporary thinkers, such as the French historian and philosopher Marcel Gauchet , democracies risk falling victim to their own success: When all citizens demand their rights but are unaware of their responsibilities, the political questions that have defined democratic life over centuriesâ€"How should we live together? What is in the public interest, and how do I balance my own interest with it? Thus the balance between privacy and transparency is especially in need of adjustment in times of rapid technological change. That balance itself is a political issue par excellence, to be settled through public debate and always left open for negotiation. In the last few decades, as we began to generate more data, our institutions became addicted. We, as citizens, are caught in an odd position: No, we release data out of self-interest, on Google or via self-tracking apps. We are too cheap not to use free services subsidized by advertising. Or we want to track our fitness and diet, and then we sell the data. Whatever the original incentive for computerization may have been, processing increasingly appears as the ideal means to adapt an individual to a predetermined, standardized behavior that aims at the highest possible degree of compliance with the model patient, consumer, taxpayer, employee, or citizen. Big data, with its many interconnected databases that feed on information and algorithms of dubious provenance, imposes severe constraints on how we mature politically and socially. The worst part is that we do not see it as such. Because we believe that we are free to go anywhere, the barbed wire remains invisible. The more information we reveal about ourselves, the denser but more invisible this barbed wire becomes. We gradually lose our capacity to reason and debate; we no longer understand why things happen to us. But all is not lost. We could learn to perceive ourselves as trapped within this barbed wire and even cut through it. Privacy is the resource that allows us to do that and, should we be so lucky, even to plan our escape route. This is where Simitis expressed a truly revolutionary insight that is lost in contemporary privacy debates: Think of privacy in ethical terms. If we accept privacy as a problem of and for democracy, then popular fixes are inadequate. For example, in his book Who Owns the Future? On this logic, by turning our data into an asset that we might sell, we accomplish two things. First, we can control who has access to it, and second, we can make up for some of the economic losses caused by the disruption of everything analog. In Code and Other Laws of Cyberspace first published in , Lawrence Lessig enthused about building a property regime around private data. Only if the machines can agree will the site be able to obtain her personal data. It would be extremely dynamic: The property regime can, indeed, strengthen privacy:

Perhaps they might pay a small fee or promise a tax credit for the privilege of nudging you later onâ€”with the help of the data from your smartphone. Consumers win, entrepreneurs win, technocrats win. Privacy, in one way or another, is preserved also. So who, exactly, loses here? We also should worry about the implications for justice and equality. For example, my decision to disclose personal information, even if I disclose it only to my insurance company, will inevitably have implications for other people, many of them less well off. People who say that tracking their fitness or location is merely an affirmative choice from which they can opt out have little knowledge of how institutions think. Once there are enough early adopters who self-trackâ€”and most of them are likely to gain something from itâ€”those who refuse will no longer be seen as just quirky individuals exercising their autonomy. No, they will be considered deviants with something to hide. Their insurance will be more expensive. Do I really want to share my data and get a coupon I do not need if it means that someone else who is already working three jobs may ultimately have to pay more?

Chapter 4 : Privacy And Technology - www.nxgvision.com

Technology has a number of social and ethical implications that cause debate and concern. One specific issue is privacy. Information technology has opened up society and decreased privacy.

Privacy concerns in the digital world Considering the full spectrum of privacy, people need to ask themselves if they are comfortable with all their characteristics in the public domain Share this item with your network: While the argument applies to some problems, it represents a very narrow way of looking at privacy, especially given the array of privacy problems mixed up in government data collection and use beyond surveillance and disclosure. Download this free guide Web security Keeping hackers at bay Many people assume that they are untouchable when browsing the web. Many people are wrong. Start Download You forgot to provide an Email Address. This email address is already registered. You have exceeded the maximum character limit. Please provide a Corporate E-mail Address. Please check the box if you want to proceed. I agree to my information being processed by TechTarget and its Partners to contact me via phone, email, or other means regarding information relevant to my professional interests. I may unsubscribe at any time. A European paper issued by Michael Friedewald distinguishes seven types of privacy: Considering the full spectrum of privacy, people must ask themselves: Are you sure you are comfortable with all of your characteristics in the public domain? For example, do you want people to know where you spend your time - and who you like to spend it with? If you called a substance abuse counsellor, a suicide hotline or a divorce lawyer? What websites you read daily? The religious and political groups to which you belong? Key privacy questions Furthermore, as big data grows, enterprises need a robust data privacy solution to help prevent breaches and enforce security in a complex IT environment. Here are five of them: Can we trust our sources of big data? What information are we collecting without exposing the enterprise to legal and regulatory battles? How will we protect our sources, our processes and our decisions from theft and corruption? What policies are in place to ensure that employees keep stakeholder information confidential during and after employment? What actions are we taking that create trends that can be exploited by our rivals? The problem is, the internet is a worldwide network and everything must be developed for a global environment without national borders. Many users approve a privacy policy without reading it, and many of these policies are vague guidelines where it is completely impossible for users to foresee the scope and content of their consent to the processing of their data. The consent to this agreement is mandatory to access the service. Consequently, users have no choice if they want to use it. Shifting privacy standards Furthermore, the service provider may change this policy. Everybody remembers the Instagram case. Due to the strong reaction, Instagram backed down. This brings to the forefront the fact that many consumers are poorly educated about how their personal data is collected by companies and are unsure about what it is actually used for. Investigation into the recent implementation of the EU Cookie Law has highlighted how misinformed consumers in Europe are. This is surprising, given that an initial warning banner appears on UK websites informing the user if the site uses cookies. This corresponds closely to the percentage of those who said they generally browsed the internet with cookies disabled. Google Glass All of this is soon to be compounded by wearable technology, such as Google Glass, which is essentially a phone in front of your eyes with a front-facing camera. A heads-up display with facial recognition and eye-tracking technology can show icons or stats hovering above people you recognise, give directions as you walk and take video from your point of view. But, crucially, this does not solve other privacy concerns. Google Glass tracks your eye movements and makes data requests based on where you are looking. This means the device collects information without active permission. Eye movements are largely unconscious and have significant psychological meanings. For example, eye movements show who you are attracted to and how you weigh your purchase options when shopping. How many of you will turn off your Glass while punching in your PIN? How about when opening your bills, filing out tax information or filing out a health form? All of this information can be compromised with a security breach, revealing both the information of the one using Google Glass and the people they surround themselves with. On 4 July , Chris Barrett, a documentary filmmaker, was wearing Google Glass for a fireworks show in Wildwood, New Jersey,

when he happened upon a boardwalk brawl and subsequent arrest. The fact that the glasses were relatively unnoticeable made a big difference: The hands-free aspect of using Google Glass to record a scene made a big difference. Intrinsic right or social construct? Privacy is entering a time of flux and social norms and legal systems are trying to catch up with the changes that digital technology has brought about. Privacy is a complex construct, influenced by many factors, and it can be difficult to future-proof business plans so they keep up with evolving technological developments and consumer expectations about the topic. One way to ensure there are no surprises around privacy is by seeing it not as a right, but rather as an exchange between people and organisations, bound by the same principles of trust that facilitate effective social and business relationships. This is an alternative to the approach of "privacy as right" that instead positions privacy as a social construct to be explicitly negotiated so it is appropriate to the social context in which the exchange takes place. Isaca notes that enterprises eager to reap the benefits of big data and its vast potential must also recognise their responsibility to protect the privacy of the personal data gathered and analysed with big data. Risk management and maintaining adequate mechanisms to govern and protect privacy need to be major areas of focus in any big data initiative. The lengthy privacy policies, thick with legalese that most services use now, will never go away, but better controls will, and should, emerge. Whatever tools are used to protect and collect personal data in the future, it will be important for companies such as Facebook and Google to educate their consumers and to provide them with options for all levels of privacy. This was last published in October Read more on Privacy and data protection.

Chapter 5 : Technology and Privacy: The New Landscape by Philip E. Agre

As technology provides us with more and more conveniences, the way we think of privacy will necessarily change. As technology improves and our desire for convenience grows accordingly, what we think of now as "privacy" may become a relic.

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.

Chapter 6 : TECHNOLOGY AS A THREAT TO PRIVACY: Ethical Challenges

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.

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.

Chapter 7 : Privacy concerns in the digital world

Just because privacy expectations are historically determined and relative, it is a fallacy to assume that they have to become weaker as technology becomes more powerful. As noted such a view is reflected in some United States court decisions.

Almost all the information these devices collect can be sold to companies or used by governments and law enforcement to keep tabs or gather evidence. At the same time, we use technology so frequently as a society because it allows us to do things faster and with much less effort. Is the trade-off worth it, or are we selling our souls to the devil? We conducted a survey to find out where public opinion lies on the question of technology and privacy or security. People of different age groups and different occupations answered questions to determine how bothersome certain devices were to them regarding privacy violations. As it turns out, some feel technology is far too convenient to give up despite its flaws, while others would trash their devices if they found out it was spying on them. Of course, many were of mixed opinion and considered these issues on a case-by-case basis. While the spectrum of sentiment on the issue is quite varied, the discussion of technology and privacy is one of paramount importance today. Continue reading to learn what we found. Health care, government, finance, and transportation industries have all had to increase their security budgets recently to prevent a rise in cyberattacks. Arts and entertainment, which has been harmed by online piracy for decades now, is also uncomfortable with criminality. Outside of more high-profile crimes in the sphere of industry, homemakers, retirees who own property, presumably , and retailers also feel threatened by cybercriminals, who have been targeting individual digital property at an increased rate over the past few years. Industries threatened by government privacy intrusion include the industries we often see battling regulation in the public eye. Responses were similarly low less than 10 percent of each gender were concerned on the questions of whether privacy intrusion bothered the person at all and whether the data should be used in legal proceedings. The low returns on these questions could be a result of the "nothing to hide" sentiment rearing its head again or a result of people finding concern in other areas of privacy violation. Much higher returns were generated on questions of tracking, conversation monitoring, and the sale of data for advertising. Women were more concerned overall with identity and location tracking. A variety of digital issues disproportionately affects women , which include stalking and location tracking by ill-intentioned people. Where men took more issue than women: It can be disconcerting to look up a new fridge only to find your Facebook and news sites flooded with appliance advertisements the next morning. Not to mention the annoyance of a sluggish website bogged down by advertisements. Privacy Through The Ages Different generations have different relationships with technology and, as such, have different concerns about specific technologies and their relationship to privacy and security. Those 65 and older appeared to be very distrustful of technology, recording higher levels of concern than younger generations in almost every field. Those in the age bracket of all found location tracking, home security, and smart device privacy issues to be the most threatening. People who fell in this age group appeared to be the least distrustful of fitness tracking devices, although they still disliked them more than younger generations. From age 18 to 44, the data trends looked rather similar. A uniform distrust of social media existed, but they regarded smart thermostats, fitness trackers, and public surveillance as less of an issue than older generations. Younger age groups may be less concerned than others about these issues because they trust businesses to keep their data secure. On the other hand, they seem to be warier of home and smart car security. Interestingly, to year-olds recorded their highest level of concern was home security. The Vice of All Devices Each device we use possesses a unique capability to compromise our privacy. Two of the top three issues involved being watched and tracked by cameras. Most people were very uncomfortable with the eerie prospect of being spied on through cameras on their TVs, though this possibility exists in webcams and smartphone cameras , as well. Interestingly, the second biggest concern involved data intrusion by anti-virus software. Taking third place was biometric facial recognition, another issue that depends on camera surveillance to succeed. Strangely, surveillance by public security cameras was among the least concerning to people. Despite social media being one of the largest data collectors of this list, less than half of those

surveyed found it to be a threat. This might be related to the growing rates of social media use over the years. People were also not quite as concerned about smart home, smart car, and smart thermostat security system hacking, and this lack of suspicion about these devices seems to jive with the high level of interest among the public in owning connected homes and cars. The Privacy Ultimatum When asked about whether privacy violations would make a person reconsider using convenient tech devices, a rather stark divide appeared between the generations. Millennials and some a few years older responded that fewer than 20 percent would forsake technology because of its intrusion into their personal life. This percentage aligns with the findings of many similar studies: In other words, younger people make the most use of technology but exhibit the least concern. The situation changed quite drastically, however, between the age brackets of 35 to 44 and 45 to This might be that year-olds are still technically millennials, and those just a few years older may have similar sentiments toward technology. Allow for one decade, though, and respondents were almost twice as likely to stop using a device that violated their privacy. The older one became, the more likely they were to adhere to this line of thinking. However, the feelings people display toward the implications these devices have on our privacy vary quite widely. Men considered these consequences differently than women did. Even people across different industries had varying thoughts about what technology was good for and what the greatest risks were of its privacy shortcomings. If anything, the wide array of opinions on privacy in the digital age is a demonstration of rising awareness among the American public. Even 10 years ago, this level of comprehension would not have existed. Finally, people of all walks of life are giving these important issues more and more thought. Methodology We surveyed 1, people aged 18 and older about their opinions on security and other electronic devices and whether they felt the risk to privacy was worth the security and convenience benefits. Using the results of the survey, we were able to segment responses based on age, gender, employment, and other demographics. The visualizations were created using the data generated from the survey. Fair Use Statement Privacy of this content is not a concern of ours, so feel free to share this page for noncommercial purposes only. Please be sure to link back to this page to give proper credit to the authors. Privacy Policy Popular Searches.

Chapter 8 : Privacy and Information Technology (Stanford Encyclopedia of Philosophy)

As Web companies and government agencies analyze ever more information about our lives, it's tempting to respond by passing new privacy laws or creating mechanisms that pay us for our data.

Chapter 9 : Privacy and Technology

The fact that privacy is expressed by means of information, implies that it is possible to distinguish different categories of privacy namely, private communications, information which relates to the privacy of a person's body, other personal information, and information with regard to a person's possessions.