DOWNLOAD PDF THE ASSAULT ON PRIVACY

Chapter 1 : Chrome 69 Is a Full-Fledged Assault on User Privacy - ExtremeTech

Comment: A copy that has been read, but remains in clean condition. All pages are intact, and the cover is intact. The spine may show signs of wear. Pages can include limited notes and highlighting, and the copy can include previous owner inscriptions.

His demand that the internet companies abandon their stance on privacy now carries the weight of the British government. Bernard Hogan Howe, the Metropolitan police commissioner, said this month that space and technology firms must do more to frustrate paedophiles, murderers and terrorists. Hannigan tells us that Islamic State Isis is bad because it tweets and makes strategic use of hashtags, like all the other small-time self-promoters out there. He is not asking for legislation or proposing legal change. Instead he is deploying the most inflammatory and misleading language available, to publicly blackmail companies into abandoning the rule of law, to bludgeon them into providing assistance for the illegal surveillance of their customers. For decades, the NSA and GCHQ bullied, bribed and bamboozled telecommunications companies around the world into providing limited assistance. The companies who knowingly cooperated did so in secret. They had no reason to expect their customers to find out. If customers did, they had nowhere else to go: If their customers want out, technology has already created higher-privacy options. The architecture of the net does not require us to use vast centralised arrays of servers and memory owned by companies in order to do our sharing with friends. With small technical adjustments at low cost, households and businesses could shift to secure and private modes of sharing and communicating that would cut out the middlemen. They will be compelled to fall back upon mechanisms subject to control by the rule of law, such as search warrants. The companies must protect their customers to the full extent the law allows them, or lose their business â€” and also must meet their obligations to law enforcement as defined by the courts of the places in which they do businesses. They cannot exceed legality in either direction without courting destruction. Hannigan, for all his blowhard rhetoric, would be infinitely worse off without them, so he must bully them into action beyond the legal requirements. Perhaps he thinks that to be free from state spying is not included in those endowments. One wonders what he thinks those ordinary Americans fought for who died to keep Yorkshire out of the Third Reich. He should be fired. Instead the bandwagon rolls on.

Chapter 2 : The Assault on Privacy: Computers, Data Banks, and Dossiers by Arthur Raphael Miller

The rules of the privacy game have changed again, and you probably didn't even notice. It happened early this month, when a federal judge ruled that a company must begin collecting information.

September 06, He was not informed of the charges against him. The police forced themselves into his house and occupied it for the next eight hours, questioning him and his wife Pavana on their dress, personal beliefs and marriage. Pavana had written to each other â€" the Telangana police read them aloud and translated them for the Maharashtra police personnel. Satyanarayana on his caste identity and Ms. They insisted that Mr. Satyanarayana keep the washroom door open and change his clothes in their presence. They barred entry to all and refused to permit the couple to step out of the house. Satyanarayana requested the police to complete the search before his daughter returned from school, to protect her from the trauma of the search, they refused to comply. Satyanarayana lost that day is incalculable. It was a daylight heist of his professional assets put together over two and a half decades â€" e-books, papers, unpublished manuscripts, course materials and teaching resources. The last straw was when the police questioned him about his reading habits, his academic practice, and why he had books on Ambedkar, Mao and Marx. When he finally got access to a Marathi translator around 5 p. Satyanarayana realised that the warrant had nothing to do with him. It only stated that his father-in-law, poet Varavara Rao , who another team of police personnel had already placed under arrest at his home, was residing with him. While they forcibly entered and searched Mr. This tells a story of the total and absolute infringement of Mr. My arguments here are immediately relevant to all those who were targeted on August 28, five of whom were arrested. Satyanarayana, all of whom are respected public intellectuals, Dalit pedagogues who have been instrumental in crafting radically new approaches to the understanding of anti-caste philosophies and have resisted the ongoing assault on higher education in enduring ways. I hope that in the context of these arrests and searches, the court will initiate a moral and material recuperation of dignity and materials in the difficult times we live in today, and uphold justice and the Constitution in the national interest. Guaranteeing dignity The core value that the judgment is built around is dignity as the right to life. How can dignity be understood? The Preamble of the Constitution states: Fraternity assuring the dignity of the individual and the unity and integrity of the nation. Sapre says in the privacy judgment: Dignity of the individual was, therefore, always considered the prime constituent of fraternity, which assures the dignity to every individual Unity and integrity of the Nation cannot survive unless the dignity of every individual citizen is guaranteed. The duty of care to be exercised by the state in its treatment of citizens is hinged on the right of citizens to be free of state intrusion and surveillance through domiciliary visits, and to be treated with care. Because free speech is facing the biggest threat in India today, Justice S. In the case of Mr. Satyanarayana then, there has been a gross violation of the sanctity of the home, marriage, expressive and cognitive freedoms, and bodily integrity through the assaultive gaze of the police even at private moments in daily routines. This violation was through surveillance, through deliberate public humiliation on the campus of an intellectual, a Dalit intellectual. What can be worse than this, and what reparations can the court order?

Chapter 3 : Privacy and Culture

But claims that "dark money" is corrupting our elections are much exaggerated. The law already requires full public disclosure of contributions to candidates, parties, PACs, and super-PACs.

These judgments are made in ways dictated by culture, upbringing, and experience. We may judge whether to share information with others based on how they are dressed, how they speak, who initiated contact, their reputation, whether they seem friendly, whether and how they are related to us, whether they are corporations or individuals, whether they seem honest, and so on. There are as many ways of judging whether to share personal information as there are people. Privacy reflects individual, cultural, and social norms that resist being catalogued. Privacy norms can also change. When we have business dealings with others, we can control by contract what becomes of the personal information we reveal. Many commercial interactions have at least implied promises of confidentiality. We give documents to a tax preparer, for example, with an implicit understanding that the privacy of personal financial information will be maintained. Like our personal interactions, almost all of our commercial interactions come with a web of cultural understandings about uses of information that is nearly impossible to describe. The rise of digital transfer and storage of information has started a worldwide discussion of what these cultural norms will be in the future. When our cultural privacy norms are violated, there are a number of things we can do. Individuals, for example, thrive on sharing information. But when gossip goes too far and a person gives too much publicity to the personal information of another, both are likely to suffer. Such incidents counsel the victim and the gossip to be more circumspect when sharing personal information in the future. This is how privacy norms are made and reinforced in personal interactions. When our cultural privacy norms are violated in a commercial context, we have remedies there, too. The most common and effective one is refusal to deal. People can easily be inconvenienced and offended when contacted for commercial purposes, and they will turn away from businesses that do this. Alienating customers is bad for business. Though they could, they recognize that this would offend customers and victims more than it would communicate newsworthy information. The commercial entity that continues to use consumer information intrusively, defying common sense and good business, can be brought to heel by other consumerist actions. Offended people can publicize the offensive behavior, for example, encouraging others not to do business with the offender. Where even that fails, there remains the possibility of common law suits for invasion of privacy. Consumers who are extremely sensitive about uses of their personal information can protect their sense of privacy and prevent those uses simply by withholding their personal information from everyone. People who pursue a high degree of privacy may find themselves solitary and isolated. One cannot maintain a high level of privacy and have full interaction with society at the same time. The trade-offs between levels of interaction and privacy, however, are ones that individuals are well equipped to make based on culture, upbringing, and experience.

Chapter 4 : The Assault on Privacy: December

Assault on privacy continues relentlessly The traffickers are getting more aggressive, and the government's not helping.

Maybe Microsoft had a point. Prior to Chrome 69, Chrome offered an optional sign-in feature. This feature had nothing to do with your various accounts on services like Gmail or YouTube â€” instead, it allowed Google to synchronize things like cookies and bookmarks across all of the devices on which you used Chrome services. Many people embraced the feature, but Google kept it opt-in. The old login icon looked like a blank outline of a person. When clicked, it displayed the following message: But now, Google has changed this message. Download and install Chrome 69, and the browser now treats this sign-in option as exercised if you log into any Google account. In other words, Google now treats the Chrome sign-in and the Google account sign-in as equivalent. There was no reason to make this change. My teammates made this change to prevent surprises in a shared device scenario. In the past, people would sometimes sign out of the content area and think that meant they were no longer signed into Chrome, which could cause problems on a shared device. The idea is that people thought they were signing out of Chrome when they were actually signing out of a content area. But as cryptographer and professor Matthew Green points ou t, this is only a problem for people who sign into Chrome in the first place. Does it mean you are synced already, or is it inviting you to initiate a sync? If a pattern is defined as a regularity in the world designed or naturally occurring that repeats in a predictable manner, a dark pattern is an attempt to trick users by designing interface options that look like the options users expect to see. Notice how the boxes work. If you want your Google Plus profile to be maximally private, you want to remove all of the check boxes from the first set of options and put a checkbox in the Photos and Videos option. First, the company trains you to expect the UI to act a certain way, then it changes the actions of the UI mid-stride so you pick the action it wants you to choose rather than your actual intended result. Google has transformed the question of consenting to data upload from something affirmative that I actually had to put effort into â€” entering my Google credentials and signing into Chrome â€” into something I can now do with a single accidental click. This is a dark pattern. Some have seen the Sync feature fully activate from clicking it once, but two-factor authentication may have been involved in that step. Hmm, in dev, I believe I just click on "sync as" in the user switcher and that turns on all sync settings â€” I get a "congrats" screen with an "undo" button. Not sure about stable. Google has also acknowledged allowing third parties to sweep Gmail for data as well. But this is unsurprising. The company establishes a mechanism by which users can opt out of something, then breaks that mechanism if too many people opt out of it. This kind of behavior is profoundly damaging to any conception of trust.

DOWNLOAD PDF THE ASSAULT ON PRIVACY

Chapter 5 : Assault On Privacy | Randy McMillan - racedaydvl.com

Starting with only his email address and without a warrant, the government used pen register and trap-and-trace devices (pen-traps) to locate Ross's home and collect all the internet traffic information flowing through his router and laptop.

Assault on Privacy Imagine if you woke up one day to find out that your medical information, social security number, home address, and banking information were in the hands of someone else. Imagine how quickly that could put you and your loved ones in danger. This may seem like a stretch for some, however, for many others this is the reality that they will face today. It is difficult to overlook the many ways in which our lives are being shaped and influenced by technology, more specifically the mass media. The world that once seemed so large and distant is now often at your fingertips and with a few key strokes one can interact, do business with, or meet someone across the world. The advancement of technology in our culture has also led to many new dangers. In this discussion, we will identify the agents of socialization, paying special attention to the mass media. We will look at how technology influences the process of socialization. Keeping this scenario and the information found in unit 2 in mind, please respond to the following prompts: What types of actions can be taken to avoid having your most personal information end up in the hands of someone who may have intentions to harm you? Use the Internet to research at least one additional article on this issue to support your responses. Calculate the price of your order The price of a paper depends on the number of pages, academic level and the urgency. To know how much you would pay for an order, fill in the basic paper details. Confidentiality and Security We take confidentially of our customers seriously. This is the reason we use only PayPal to make payments that require only an email. Our website is also encrypted to ensure additional security. In addition, we never sell your paper nor divulge the paper or client details to anyone. Authenticity We write all our papers from scratch and never plagiarize at all. You are guaranteed of a custom-made non-plagiarized paper that you cannot find anywhere else even in part whenever you order from us. Professionalism Professional writers in the various fields who have a wealth of experience in academia write all your papers. You are, therefore, guaranteed of a well-researched paper with the right content and in the correct structure. Our services are legal and acceptable Do you know that it is legal to seek our academic writing services and is not against the policies of your university, college or any other learning institution? You are not prohibited from getting our custom-made papers if you use them in any of the following ways; As a source for additional understanding of the subject As a source of ideas for your research, in this case, it should be properly referenced For proper paraphrasing as per your schools plagiarism definition and acceptable paraphrase Direct citing in your work, when properly referenced.

DOWNLOAD PDF THE ASSAULT ON PRIVACY

Chapter 6 : Assault on Privacy | The History Of Big Data

However, things soon became more complicated when the vice-principal discovered text messages on the phone about a recently stolen vehicle. Because of the illegal activity involved, the vice-principal contacted and handed the matter over to police.

The emerging mobile industry is expected to be characterized by increasingly personalized and location-based services. Among these services, personalized mobile marketing and advertisement services are predicted to be particularly important. However, besides the excitement about the potential innova There is indeed a thin line between providing useful services and bombarding the user with mobile spam. Conscious of the importance of solving this sensible issue, the mobile marketing association itself has issued privacy guidelines to its members. However, because this self regulation has proven weak in protecting users from abuses, regulatory bodies throughout the world have issued laws to protect user privacy. This paper illustrates and compares the regulatory frameworks of Switzerland, the European Union and the United States, and analyzes their likely implications for the mobile business industry. Show Context Citation Context We investigate legal and philosophical notions of privacy in the context of artificial agents. Our analysis utilizes a normative account of privacy that defends its value and the extent to which it should be protected: We argue that the fact that the only entity to access my personal data such as email is an artificial agent is irrelevant to whether a breach of privacy has occurred. What is relevant are the capacities of the agent: The system relies on credits and blacklists, with each protected device periodically requesting new credit in order to continue operating. The client part is a hybrid system consisting of an untrusted software component and a trusted hardware component. This offers maximum flexibility, while keeping the hardware requirements low. A variety of theft-protection methods already exist, see Fig. They can be combined to increase the level of protection. Wireless signals can be used to prevent devices equipped with such transmitters from being removed from protected premises [1]. In contrast to physical locks, tracking is transparent to the user. Passive tracking systems, such as serial number registries, are easy to install,

Chapter 7 : CiteSeerX â€” Citation Query The Assault on Privacy

The assault on privacy: computers, data banks, and dossiers Item Preview remove-circle Share or Embed This Item.

Chapter 8 : Editorial: The assault on privacy

Having failed to secure a bill outlawing the encryption of private data, the FBI and Justice Department are now "engaged in a multi-pronged attack on all sorts of other privacy rights â€” this.

Chapter 9 : Assault on Privacy â€” Free Ross

Justice R.F. Nariman observed that of the three aspects that are at the core of the fundamental right to privacy, "the privacy of choice, which protects an individual's autonomy over.