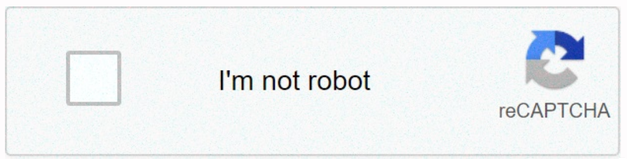

Continue

Dragnet nation pdf

Online ads of websites you've visited... Smartphones and cars that transfer your location... Monitor data collection over the Internet and over your phone lines. They are being watched.... Angwin offers a revealing and troubling look at how the government, private companies, and even criminals use technology to indiscriminately sift through vast amounts of our personal data. She argues that the greatest long-term danger is that we start internalizing surveillance and censoring our words and thoughts until we lose our freedom. Horrified by such a perspective, Angwin conducts a series of experiments to protect himself. We see online ads from websites we have visited long after we have moved on to other interests. Our smartphones and cars transfer our location so we know what's in the neighborhood, but also others to track us. And the federal government, as we recently learned, has carried out massive data collection surveillance over the Internet and over our telephone lines. In Dragnet Nation, award-winning investigative journalist Julia Angwin reports on the front lines of the American surveillance economy, providing a revealing and troubling look at how the government, private companies, and even criminals use technology to indiscriminately scour vast amounts of our personal data. In a world where we can be observed in our own homes, where we can no longer keep secrets, and where we can imitate, financially manipulate, or even put ourselves in a police station, Angwin argues that the greatest long-term danger is that we will begin to internalize surveillance and censor our words and thoughts until we lose our freedom. , which makes us unique individuals. Horrified by such a prospect, Angwin is conducting a series of experiments to protect himself, from quitting Google to wearing a burner phone, showing how difficult it is for the average citizen to resist the trawl's reach. Her book is a cautionary tale for all of us, with profound implications for our values, our society, and our self. --Publisher information. Dragnet Nation: A quest for privacy, security and freedom in a world of relentless surveillance AuthorJulia AngwinCountryUnited StatesSubjectComputer and Network SurveillancePublisherTimes BooksPublication datum25. February 2014Pages304ISBN978-0805098075 Dragnet Nation: A quest for privacy, security and freedom in a world of relentless surveillance is a 2014 book about computer Network monitoring by Julia Angwin. The author said she was motivated to write the book when she learned of data scratches. [1] Reception Various commentators have reviewed the book. It has generally received good reviews. [2] [3] [4] References: Sharma, Neha (26 February 2014). Reclaiming Privacy in An Age of Hyper-Sharing. kirkusreviews.com retrieved January 28, 2015. Staff (1 March 2014). 2014). Privacy: Observe the Observers. economist.com. Retrieved January 28, 2015. Staff (25 February 2014). DRAGNET NATION by Julia Angwin. Kirkus reviews. Retrieved January 28, 2015. * Silverman, Jacob (March 6, 2014). 'Dragnet Nation' looks at the hidden systems that always look at you - LA Times Los Angeles Times. Los Angeles: Tribune Co. ISSN 0458-3035. Retrieved January 28, 2015. External links Official website video interview of the author and Bill Moyers This article about a book on the Internet is a stub. You can help Wikipedia by expanding it.vte Retrieved from In another addition to the genre Do Something for a Year and Then Write a Book About My Experiences follows Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance Julia Angwin's years-long search for a semblance of online privacy. The author talks about her attempt to minimize at least the ubiquitous surveillance of big business, and concludes early on that it is almost impossible to escape the whole of intrusive online views. (Spoiler: It usually fails.) The book highlights the difficulties of maintaining privacy in an online-centric world, even for a computer-savvy, well-connected Pulitzer Prize winner like Angwin. The author's message is clear: if something is free online, like many of our favorite services, you are not the customer, you – and even more succinctly, your personal information – is the product. With every online click that is fed to greedy advertisers, it is unlikely that you will be able to successfully keep this product away from those who are actively looking for it. Therefore, the title – which refers to relatively indiscriminate police methods of capturing criminals – is intended to provoke the idea that companies that feed on big data indiscriminately scour the Internet for any useful information about consumers. As the author notes, the technology has enabled a new era of charged dragnets that can collect huge amounts of personal data with little human effort. And just as innocents are often caught in police trawls, so many of us are caught in online dragnets to get personal and useful information. Even the few who are most committed to online privacy among us are unlikely to be able to maintain anonymity in full while maintaining some kind of online presence, not least the general public. For those of us who would like to consider some protective measures, the author's well-researched book offers at least a general where many of the potential privacy gaps exist within our daily online interactions. To this end, the book offers a lot of good advice and discussions about online privacy online privacy how to work to preserve it. And while it contains descriptions of some of the current relevant software for maintaining privacy and anonymity online, unfortunately given the speed of innovation in the software sector, many of the programs described may be outdated or no longer available before the book is published in paperback. And as computing power inexplicably advances along Moore's predicted path, as data storage becomes cheaper and mining data processing algorithms become more advanced, we are likely to see a growing trend toward further and more extensive online intrusions into online privacy that go beyond those described in the book. Despite technological progress, we have no one to blame for much of this predicament, but ourselves. The joke that the FBI could not have wanted a better surveillance tool than Facebook has more than just a true ring. As a society, we have quickly fallen back into a situation where we post our most personal and intimate ideas online, sometimes in the form of images and sometimes in the form of text – often in 140 characters or less. Data mining algorithms and methods are advancing to such an extent that at least one trader could predict a customer's pregnancy even before she knew she was pregnant, based on her collective data on customers' regular shopping habits. Thus, the exposure of the banality of our lives through social media has not only directly undermined our privacy, but has also resulted in enough information to be freely and easily accessible about us, that even the things we still consider worthy of privacy can be extracted and dismantled by what we have made publicly available, and even de-anonymised. A social media site is able to extract gender, religious affiliation, political belief and other relatively private data from your up-voting history. A group of researchers was able to cross two social media pages and extract the identities of anonymous posters. It is important to remember that the Internet does not forget. Once you've posted something –and on some social media sites, even if you type, delete, and never really post – your pictures, words, and actions are all saved and maybe even cataloged somewhere. As employers review not only your RESUME, but also your online and social media presence, young people who grew up with an active social media lifestyle are only now beginning to understand the consequences of bad posting decisions. Regret. And even more outrageous than publishing our information there so that it can be dismantled and analyzed, the general laissez-faire attitude of the public to computer security creates further gaps in our online privacy for the data we still want to hide. Any security/data protection infrastructure is only as secure as its weakest link; we are this connection, and we definitely not safe. As the author pointed out in her book, we use weak and/or obvious passwords; We tend to use a weaker security infrastructure, if at all, because it's easier to implement, and we're often gullible enough to respond to phishing expeditions, click on fake links, and provide our passwords and other data. It is not only your personal or financial data that is at risk of exposure. Because medical data, especially genomic data, goes online and patients continue to live together on disease-oriented social media sites, even data with seemingly anonymous identifiers can be traced back to the individual. Back to the dragnet images, the issue of online privacy, especially with regard to the fourth constitutional protection of the US Constitution against baseless search and seizure, has recently reached the Supreme Court. In U.S. v. Wurie and Riley v. California, both of which were recently decided on April 29 and likely by the end of June this year, the judges struggled to establish rules and guidelines for allowing baseless searches of cellphones and smartphones as part of an arrest. Like a dragnet that catches even innocent bystanders, a seemingly innocuous police stop for a broken taillight could lead to police invading our online privacy, including access to intimate images, medical, financial, and even GPS information about a baseless search of our smartphones. In the author's case, police may not have found much on her burner phone, which is loaded with password-protected, slow data protection software wrapped in Tinfoil, in a Faraday cage with Wi-Fi turned off and a masked phone number. Or, if we remember that their experiments with the privacy of mobile phones (theirs) were by far the greatest failure, we should work to ensure that our governments enact laws and regulations that promote sensible and responsible collection of our data and protect our privacy – rather than protecting it. Privacy.