aculty of Computer & Information Sciences
Ain Shams University
Subject: Professional Ethics & Legal Aspects
Year: (2nd year) undergraduate
Academic year: 2nd term 2019-2020

Research Topic (2)

Title: The Ethics of Privacy Protection

Introduction

Privacy is your right to control how data about you is utilized, prepared, put stored, or shared. It’s also a basic right, fundamental to self-governance and the security of human dignity. If you ever go on the web, web security ought to be probably the greatest concern. Surf the web and you cannot help yet discover another tale about how much your own data is gathered while you make the most of your preferred sites.

Information privacy is a combination of: (Ref. 1)

1. **Communications privacy:**
   Ability to communicate with others without being monitored by other persons or organizations
2. **Data privacy:**

   Data privacy identifies with how a snippet of data or information ought to be handled and taken care of dependent on its relative significance and importance.

   For example, you likely wouldn't see any problems with sharing your name with an outsider during the process of presenting yourself, yet there are other data you wouldn't share with anyone until you become progressively familiar with that individual.

   The bottom line,

   Data privacy is the ability to limit access to one’s personal data by other individuals and organizations so as to have a large degree of control over that data and its use.

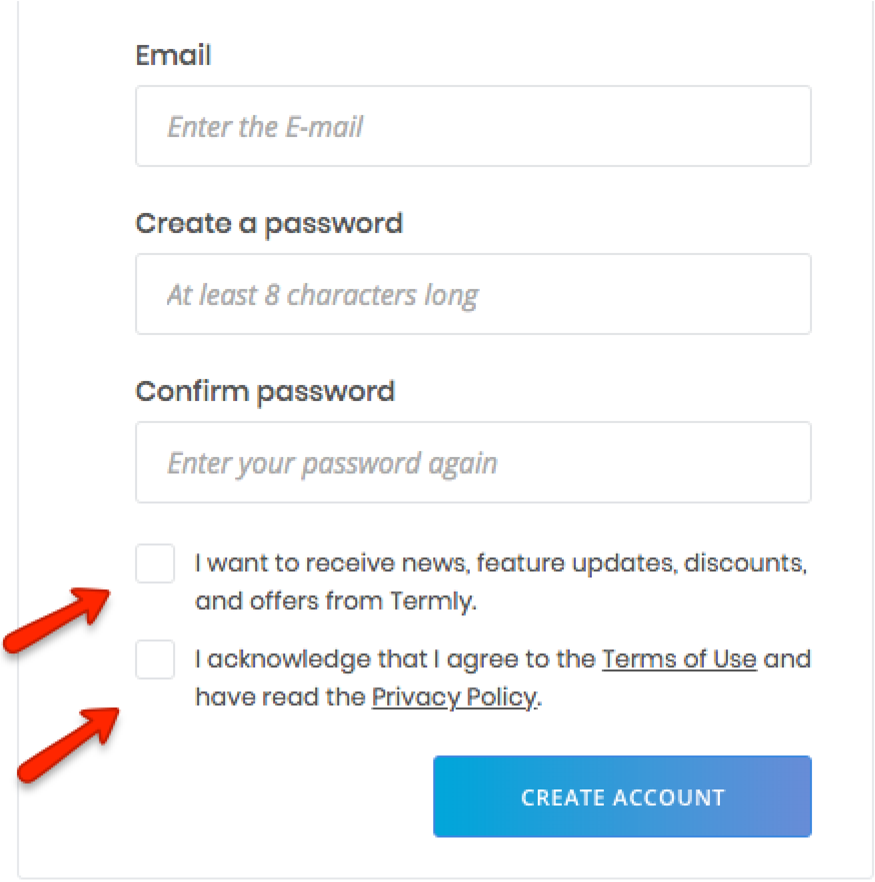
What’s Data Collection? (Ref. 2)

Data Collection is the systematic approach to dealing with and measuring facts, statistics and data from a variety of sources to get a total and exact image of an area of interest. Data collection empowers an individual or organization to respond to relevant inquiries, questions, evaluate results and make expectations about future probabilities, patterns, and trends.

A Comparison between data collection policies: (Ref. 3)

Opt-in Policy	**Opt-out Policy**
is the process used to describe when a positive action is required to subscribe a user to a newsletter list, for example.	means that a user can be signed up much more easily and he needs to be given the possibility to opt-out easily
Organization must obtain specific permission from consumers before collecting any data.	Organization assumes that consumers approve of companies collecting and storing their personal information.
Favored by consumers.	Favored by data collectors.

Example of Opt-in policy:



Email

Enter the E-mail

Create a password

At least 8 characters long

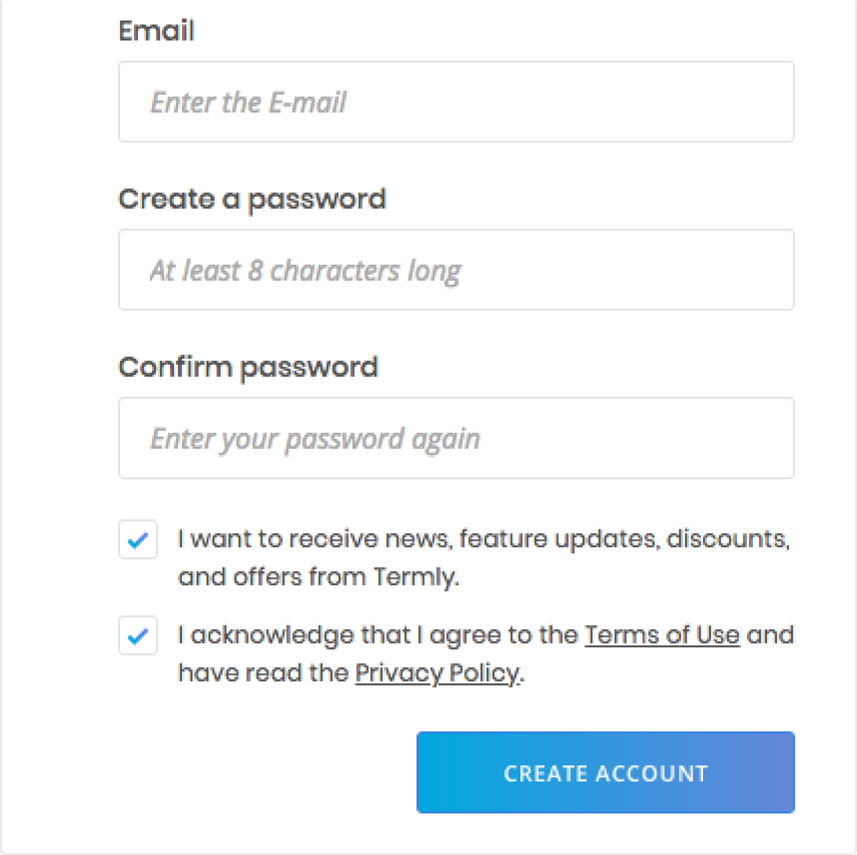
Confirm password

Enter your password again

□ I want to receive news, feature updates, discounts, and offers from Termly.

□ I acknowledge that I agree to the Terms of Use and have read the Privacy Policy.

Example of Opt-out policy:



Email

Enter the E-mail

Create a password

At least 8 characters long

Confirm password

Enter your password again

☑ I want to receive news, feature updates, discounts, and offers from Termly.

☑ I acknowledge that I agree to the Terms of Use and have read the Privacy Policy.

With opt- in, consumers must explicitly consent to third-party uses of personal data they wish to permit. In line with empirical evidence already referred to in the Introduction, we make the simplifying assumption that consumers find it too costly to opt in. As a result, all consumers prohibit that personal information about their purchasing patterns from related industries becomes publicly available. Firms therefore lack specific information about consumers before competing in the first period.

The opt-out system gives a consumer the option to stop sharing of its non-public information. As in reality very few consumers do exercise this option, we model that consumers do not opt out. An explanation for this consumer behavior is that opting out may be too costly to do, consumers are unaware of this option, or may not find it beneficial to exercise the option. Therefore, consumers make available non-public information through their past .purchasing patterns at other firms.

What does GDPR stand for? (Ref.4) (Ref. 5)

GDPR stands for General Data Protection Regulation. It's the core of Europe's digital privacy legislation.

How did it come about?

In January 2012, the European Commission set out plans for data protection change over the European Union so as to make Europe 'fit for the digital age'. Very nearly four years after the fact, agreement was reached on what that included and how it will be authorized. (GDPR) law was issued in 2016 and strongly activated in May 2018.

What is GDPR?

At its core, GDPR is a new set of rules designed to give EU citizens and residents more authority over their own data. It aims to ease the regulatory environment for business so both citizens and businesses in the European Union can completely benefit from the digital economy. It unifies the regulation within the EU.

Understanding the importance of GDPR: (Ref.4) (Ref. 5)

Internet behavior has hugely changed. People send messages and emails, make bill payments, and shop online, entering personal details without even reconsidering and thinking twice. You can't agree more with this when you analyze how much personal information you may have shared. or where these details go. The data here refers to contacts, IP address, social media updates, banking information, online networking, and the history of the websites you browsed. The companies and organizations claim that they require these things to improve their customer service by being generally relevant, helpful, and useful. But does it have any facts? To address this inquiry and the concern, a new General Data Protection Regulation (GDPR) came into place.

The importance of GDPR:

The introduction of GDPR has immensely affected the way your business gathers, stores, and applies customer data today. One of the studies shows that only 20% of the companies hold fast to the new policy, while the majority of the small companies and even 60% of the tech companies haven't done anything concrete in this field. But not following the data protection rules can be harmful and destructive to your business, be it travel, retail, or tech-related. The new companies (startups) also cannot remain safe from their clutches. If you don't want to risk your business, then become GDPR agreeable.

Real life examples that happened because companies didn’t protect the user privacy: (Ref. 6)

1. **eBay**
   Date: May 2014
   Impact: 145 million users
   Details: eBay reported that an attack uncovered and exposed its whole account list of 145 million users in May 2014, including names, dates of birth, addresses, and encrypted passwords. The CEO of eBay said that hackers utilized the credentials of three corporate employees to get to its network and had total access for 229 days—more than enough time to compromise the user database.

   The company requested that clients change their passwords. Financial information, such as Mastercard number and other credit cards, was put away independently and was not compromised. The company was criticized at the time for a lack of communication with its users and poor execution and implementation of the password-renewal process.

2. **LinkedIn**
   Date: 2012 (and 2016)
   Impact: 165 million user accounts
   Details: As a significant and major social network for business experts and professionals, LinkedIn has become an attractive suggestion for attackers that looking to direct social engineering attacks. However, In the past LinkedIn has also fallen as a victim to leaking user data.

   In 2012 the company reported that attackers took around 6.5 million unassociated passwords (unsalted SHA-1 hashes) and posted them onto a Russian hacker forum. However, the attacks didn't end until 2016, the full extent of the incident was revealed. The same hacker selling MySpace’s data and was found that hackers were offering the email addresses and passwords of around 165 million LinkedIn users for just 5 bitcoins (around $2,000 at the time). LinkedIn recognized that it had been made aware of the attack, and said it had reset the passwords of influenced accounts.

3. **NetEase**
Date: October 2015
Impact: 235 million user accounts
Details: NetEase is a supplier of mailbox services through the likes of 163.com and 126.com. It was reported in that email addresses and plaintext passwords of some 235 million accounts from NetEase clients were being sold using a dark web marketplace vendor called DoubleFlag. A similar seller was additionally selling data taken from other Chinese giants, for example, Tencent's QQ.com, Sina Corporation, and Sohu, Inc. NetEase has reportedly denied any penetrate. HaveIBeenPwned lists this penetrate as "unverified".

Conclusion

Data is the core of current generation and backbone of companies. Your data is so useful and other companies may pay a lot of money to get it. So make your huge efforts to protect your data. When our data are wasted, our reputation can be corrupted. And as I explained in the research Data privacy , Data collection with its types, GPDR and some issues that happened as a result the lack of protection from some companies. So my advice to you is to **Be Careful** with your data !

References:

[1] LifeLock (Website): Link
[2] TechTarget (Website): Link
[3] Termly (Website): Link
[4] ZDNet (Website): Link
[5] Lander (Website): Link
[6] CSO (Website): Link
[7] "Ethics in Information Technology 5th Edition" (Book): Link.