

Privacy dark patterns in identity management

Lothar Fritsch¹

Abstract: This article presents three privacy dark patterns observed in identity management. Dark patterns are software design patterns that intentionally violate requirements, in the given case privacy requirements for identity management. First, the theoretical background is presented, and then next, the observed patterns are documented, described and formalized. The resulting dark patterns show how security is used as obfuscation of data collection, how the seemingly harmless collection of additional data is advertised to end users, and how the use of anonymization technology is actively discouraged by service providers.

Keywords: privacy patterns, dark patterns, identity management, identity attribute extraction, dark patterns, GDPR

1 Introduction

Re-usable design patterns for privacy [LFH17] have often been proposed as a means to re-use solutions for privacy issues when implementing information systems that process personal data. Patterns are expected to increase efficiency. Undesirable patterns are called anti-patterns [DG13], which shall document frequently seen problematic solutions, and which propose generic solutions to these problems. Finally, dark patterns are a class of patterns that do have a hidden agenda, or a malicious intent to reduce privacy [Bö16]. Dark patterns are used to document techniques, designs and processes that intentionally bypass privacy. In this article, I will present observations made on web platforms which I formulate into three new dark patterns effective against privacy.

In privacy theory, anonymous or pseudonymous access to on-line services is a precondition for privacy. Direct person-relatable data such as digital identities and the respective identifiers are often collected along with other personal data by services, which is known to cause privacy risks [PF11]. Therefore, the handling of digital identities, the identification of legitimate users, and the concealing of identities are basic building blocks of on-line privacy. In spite of a number of practical solutions [Ro12], however, pseudonymous or anonymous access is not accepted by service providers. This article presents how digital identities are a target for dark patterns deployed against user privacy. Dark patterns may prove useful for upcoming compliance audits upon the implementation of the new EU General Data Protection Regulation (GDPR) [GD16s].

¹ Karlstad University, Universitetsgatan 2, 65637 Karlstad, Sweden, Lothar.Fritsch@KAU.se

1.1 Identification and Partial Identities in Identity Management

In privacy theory, a digital identity is often defined as an identifier with related identity attributes attached [CI05]. Pfitzmann and Hansen [PH10] defined:

An identity is any subset of attribute values of an individual person which sufficiently identifies this individual person within any set of persons.

They point out that there rarely is a single identity for a person, but many combinations and permutations of identity attributes that are used in various sets. Therefore, they introduce the concept of a partial identity by defining:

A partial identity is a subset of attribute values of a complete identity, where a complete identity is the union of all attribute values of all identities of this person.

The concept of the partial identity is then used to define relationships between identity and attribute data as well as relationships between sets of attributes. The authors define anonymity, unlinkability and unobservability properties based on the concept of partial identities. An important observation is that a person may become more linkable when more identity attributes are known and combined with each other.

1.2 Dark Patterns against Privacy Design Strategies

Privacy design strategies have been suggested by Hoepman [Ho14] as a means of supporting developers with the implementation of privacy. In a refinement, Colesky et al. [CHH16] extend the strategies with tactics and suggest a process that helps translating the eight privacy design strategies (MINIMIZE, HIDE, SEPARATE, AGGREGATE, INFORM, CONTROL, ENFORCE, DEMONSTRATE) into privacy mechanisms.

In their conceptualization of privacy dark patterns, Bösch et al [Bö16] specify eight antagonist strategies against the privacy design strategies (MAXIMIZE, PUBLISH, CENTRALIZE, PRESERVE, OBSCURE, DENY, VIOLATE, FAKE). These strategies are used to identify and classify privacy dark patterns.

Fig. 1 shows how the dark strategies are positioned against the respective privacy design strategies.

Bösch et al. [Bö16] then describe these dark patterns based on the application of dark strategies: *Privacy Zuckering, Bad Defaults, Forced Registration, Hidden Legalese Stipulations, Immortal Accounts, Address Book Leeching, Shadow User Profiles*. Three of these dark patterns are directly related to identity management: *Forced Registration, Address Book Leeching, and Shadow User Profiles*.

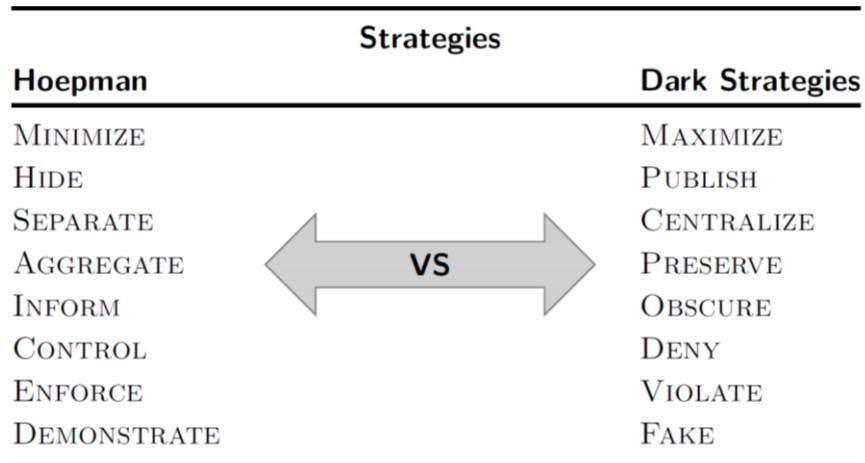


Fig. 1: Dark strategies that act against privacy design strategies (diagram quoted from [Bö16]).

2 Dark Patterns

This section describes observations made through using on-line services that constitute privacy dark patterns. The observations are documented, described, and then formalized into the dark pattern template provided in [Bö16].

2.1 Fogging identification with security

Services that require user profiles or accounts regularly use low-assurance identity management to attract users, and to keep identity management cost low. However later, when new business opportunities arise from identifying the users, services may deploy hidden identification tactics to enrich their databases, and to link their collected end user profiles to higher-assurance identities. One common tactics observed is the promise of more security for providing identifying information Figure 2 and Figure 3 show instances of this tactic observed on the social media sites Google and Facebook.

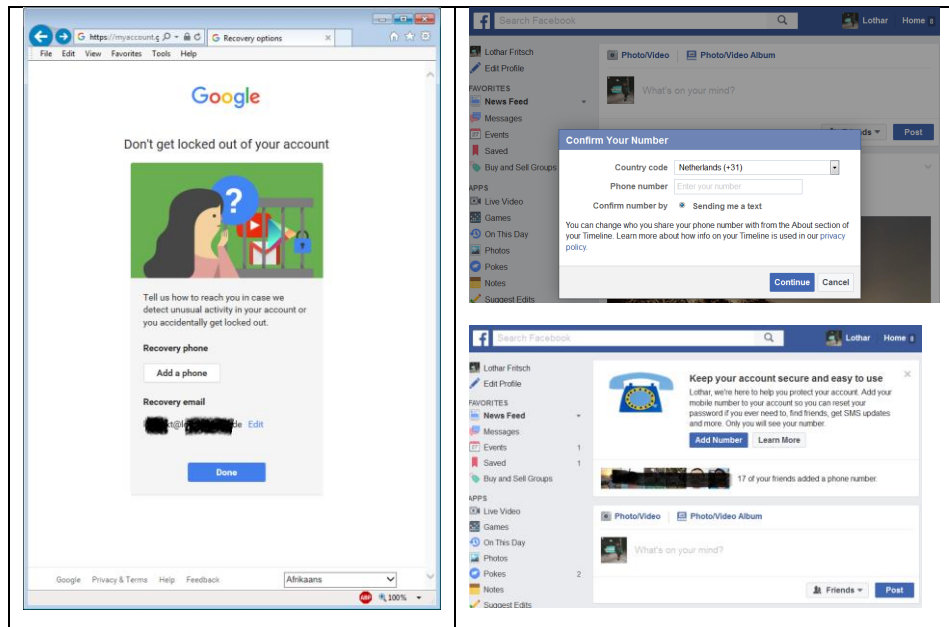


Figure 2: Phone number collection tactics. Left: Google request (20170411), upper right: Facebook request including SMS verification (20161027), lower right: Facebook request (20161027) applying social pressure with "17 of your friends have added a number".

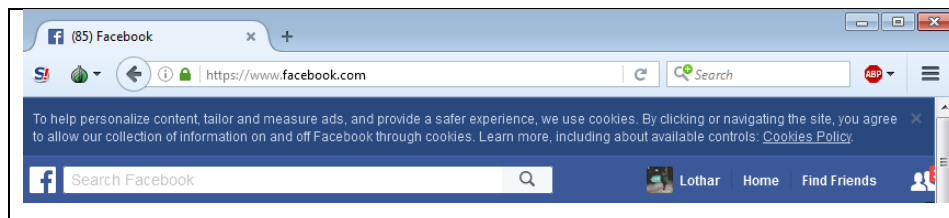


Figure 3: Collecting consent for tracking for "a safer experience" on Facebook (20161111).

Name/Aliases: *Fogging identification with security.*

Summary: While asking for identity attributes, the requesting data collector obscures the purpose of the acquisition of additional identity attributes by claiming increased security for the contributing user.

Context: On-line social media, apps, and general on-line services with user profiles or user accounts deploy this dark pattern.

Effect: The application of this dark pattern leads to increased availability of identity attributes formerly unknown. This decreases user anonymity and pseudonymity, and increases tracking, profiling and surveillance potential. The user is fogged with security

promises, and is left unaware of increased identifiability.

Description: In situations where users are under time pressure, or when they just have entered or renewed passwords, updated elements of their on-line profiles or placed orders, services use the opportunity to request additional information, or to collect consent. In particular after e-mail password renewal, requests for mobile phone numbers with SMS verification are frequently seen. The requested identity attributes usually complement the data already present in the user profiles. In some cases, the data requests can be bypassed; however, they re-appear frequently upon the next interactions with the user. Consent for cookie-based profiling is requested “for safety”.

Countermeasures: Concerning the collection of identity attributes, bypassing the request by using the often present “skip”, “later” or “cancel” options is the easiest countermeasure. Services that insist on data entry could be presented with made-up, fake or honeypot data (e.g. an unregistered prepaid phone card number used as a sink). Active collaboration to sabotage data aggregation by using other people’s random phone numbers from the phone book can be considered as an offensive countermeasure. Harvesting consent for cookie-based profiling is countered easily through cookie deletion (e.g. after closing a session window), or by deploying cookie management software within web browsers. Countermeasures that are more offensive include trading cookies with other persons to sabotage the collector’s databases with entropy (e.g. using the Cookie Cooker [Fr07]).

Examples/Known Uses: This dark pattern has frequently been seen when logging into services provided by Google and by Facebook. Screenshots are presented in Figure 2 (acquisition of identity attributes) and **Fehler! Verweisquelle konnte nicht gefunden werden.**Figure 3 (fishing for consent to place tracking cookies).

Related Patterns: *Forced registration, shadow user profiles.*

Psychological Aspects: By claiming a positive effect (more security or safety), users are pretended a positive intention of the data collector. Additional nudges [Aq12] such as listing the number of Facebook friends who already registered their phone number create group pressure.

Strategies: MAXIMIZE, CENTRALIZE, OBSCURE.

2.2 Sweet seduction: Collection of “optional” identity attributes

Service providers keep asking for more identity attributes that may not be necessary to use the services. Upon being presented with the request for information, users are promised that information is either not shared, not used, or that users have choices to deactivate usage or sharing of the recently entered information. This dark pattern has a relationship to the *Privacy Zuckering* dark pattern [Bö16].

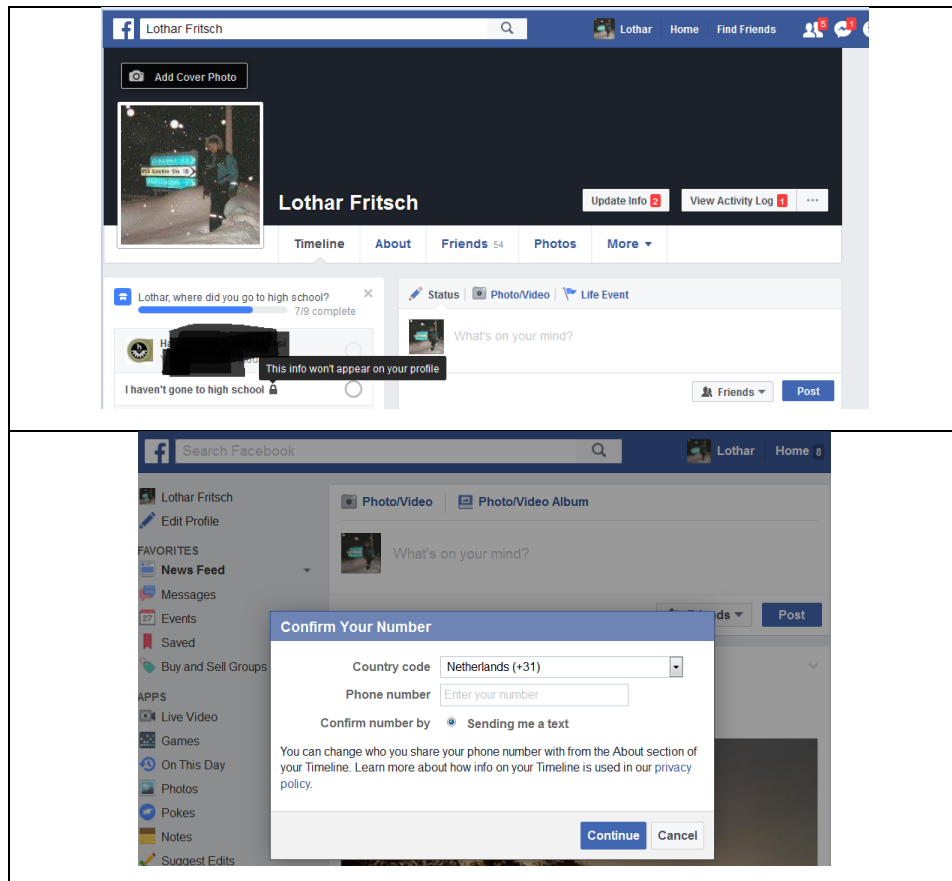


Figure 4: Top: Facebook requesting information on school visit "not to appear on profile" (20170513). Bottom: Facebook requesting verified phone number – sharing status “can be changed later” (20161027).

Name/Aliases: *Sweet seduction.*

Summary: On-line services ask for additional personal data that is not necessary to interact with the service. The requested data is promised to remain “invisible”, or alternatively to remain governed by end user policy. The newly entered information is used to amend user profiles, and to pursue more targeted business (which is not mentioned on the collection screen).

Context: The pattern has been observed as part of on-line social media that base their user identity management on profiles that collect identity attributes.

Effect: The pattern collects further identifying personal data from users. Through bogus promises, users may submit more personal data than necessary to interact with the service.

By placing the privacy management burden as an opt-out self-management duty on the user, the data most likely never will be governed by a solid privacy protection policy.

Description: Through frequent requests for additional personal information such as identity attributes, while at the same time being presented with promises of secrecy or control, data processors complement and elevate their partial identities about their users with new attributes, which in turn then will be used to amend the social graph. The purpose of the data collection is not elaborated sufficiently from a data protection perspective.

Countermeasures: The principal countermeasure is not to provide identity attributes or any other personal information when confronted with an optional request of unclear consequences. Alternatively, for obscuring one's own profile, the entry of dummy or sabotaging information can be deployed in contexts where automated decision-making on the service side that considers such information will not hurt the end user.

Examples/Known Uses: **Fehler! Verweisquelle konnte nicht gefunden werden.** shows how Facebook applies the *Sweet seduction* pattern. Users are motivated to reveal their school information to Facebook while being promised that the information remains invisible. Upon requesting verified phone numbers, Facebook promises the user governance of how the phone number is used with an opt-out model.

Related Patterns: *Privacy Zuckering, shadow user profiles.*


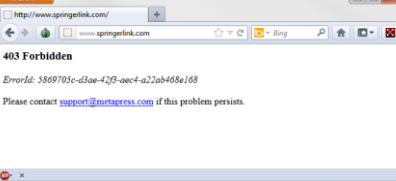

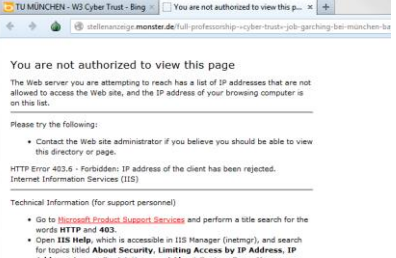
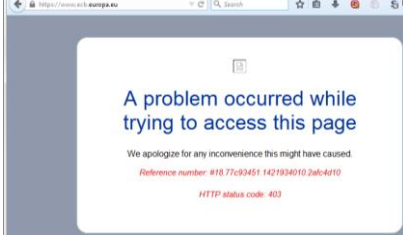
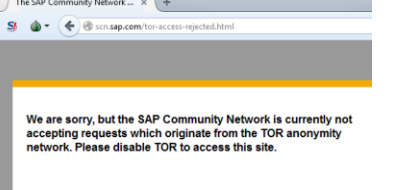
Psychological Aspects: Two major mechanisms are seen: Playful extension of the digital identity by providing additional dimensions of one's identity, and side-channelling as a footnote to another request that conceals the consequences of data collection.

Strategies: CENTRALIZE, OBSCURE, MAXIMIZE, PUBLISH

2.3 You can run but you can't hide: Enforcing network identity

One of the principal tools of identity protection is the deployment of the TOR anonymizer technology [DMS04] when accessing services on the Internet. TOR conceals the IP address and other specific network-related identifying information disseminated by a user device. User sessions appear to come from so-called TOR exit nodes, which are a number of different computers placed in many countries. Using TOR does not only hide IP addresses, but in addition prevents re-identification through IP address, but in addition prevents location look-up through Geo-IP services, and prevents correlation of IP addresses with other identity attributes (e.g. combining the known Wi-Fi IP addresses of an international airport with cookie data). In recent years, frequent users of TOR browsers have noticed an increasing number of on-line services that refused servicing connections through TOR exit nodes. Sanctions ranged from simple "unable to connect" via random error messages, direct lies about service denial up to actually admitting blocking anonymous usage. Again, security was given as the principal justification for the sanctions. On occasion, the sanctions would hit persons running TOR nodes on their own

computers, which caused the blocker to confuse non-anonymous browsing sessions with TOR sessions. The following situations were encountered using TOR to access web services. To assess actual availability of the web services, parallel access through a regular browsers, and where necessary, through a VPN to a different exit IP address were used.

 <p>The server hosting the EU privacy directive refusing to service anonymous web surfing through TOR. 5-Jul-2012, 11:36.</p>	 <p>Springerlink.com reaction on access through TOR. 9-Jul-2012, 11:32</p>
 <p>Moneybookers/Skrill refusal to accept customers from IPs that run TOR nodes. 5-Jul-2012, 11:56. Discovered upon credit card clearing refusal with an order with an online shop.</p>	 <p>Job market Monster.de refuses access to a professorship announcement in Cybersecurity. Accessed 11-Sep-2012, 13:33.</p>
 <p>European Central Bank, 22.1.2015, 14:41, with TorBrowser.</p>	 <p>The SAP community excludes TOR users. 22.1.2015, 15:26.</p>

Geocaching.com rejects a non-torified browser running on a PC that runs a TOR relay (non-exit node) in a private network with an exit node on another machine.
24.12.2014, 13:44

2015 TIMMS study results on school performance were presented to the public. To the non-anonymous public, to be precise. 29-Nov-2016. 12:06.

Skype auto-charge of prepaid account worth 80 NOK (10 €) failed on 26.6.2014, even though Skype is not being used through TOR. A TOR Relay is running on the same machine. Note reason 3 in the list.

Google.de on 7.Nov.2016 denying
access for TOR exit nodes.

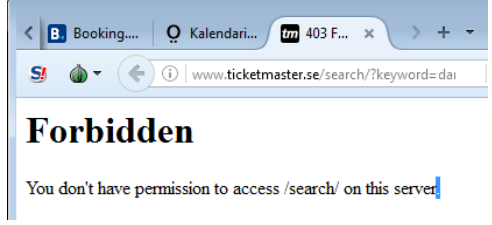
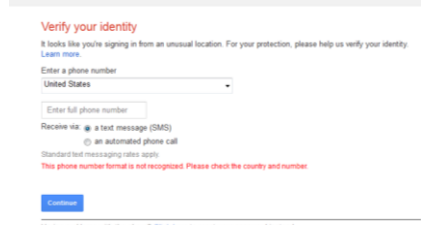
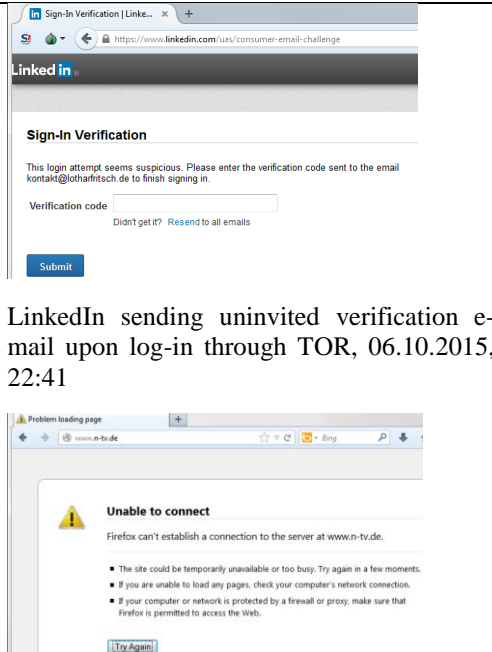
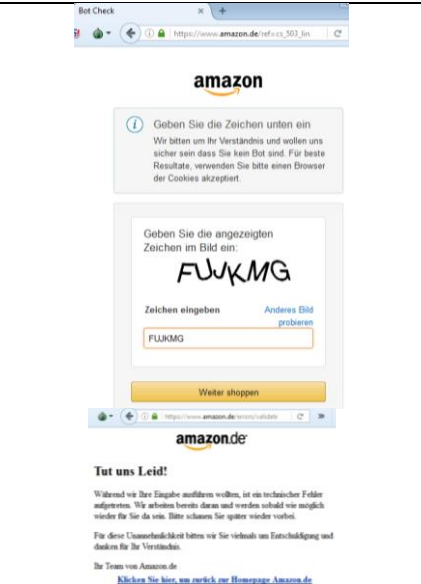
 <p>Ticketmaster.se ticket web shop, Dec 5, 2016, 9:54.</p>	 <p>Blogger.com asks for phone identification when used with some TOR nodes. 16.08.2013, 11:49</p>
 <p>LinkedIn sending uninvited verification e-mail upon log-in through TOR, 06.10.2015, 22:41</p> <p>German news TV channel N-TV blocks traffic from TOR at router level. 07.03.2014, 10:55</p>	 <p>Amazon.de requires Captcha from TOR users, then denies access explained with "technical error". Repeated effort. 2016-11-23, 15:33</p>

Figure 5: Examples of the You can run but you can't hide pattern. Listed pages have been accessed through regular browsing in parallel to ensure they were functional

Name/Aliases: *You can run but you can't hide.*

Summary: Access to services is denied based on the fact that the accessing IP address is

a known TOR exit node. The reason for denial is provided, or random error messages are given. Occasional multi-factor authentication is requested.

Context: This dark pattern is observed with e-commerce web sites, government web sites, payment web sites, blog web sites and many other on-line service providers.

Effect: The deployment of this pattern has two consequences. First, users are denied service and may not be able to access services. Second, if they are in need of the service, they may switch to a regular web browser, thereby revealing several identity attributes such as their IP address, their location, their area, the context they reside within, and other data. Revealing these identity attributes is forced upon the users without an opt-out option other than restraining from using the services, which in case of government services may not be an option.

Description: Services maintain a list of TOR nodes. Upon receiving a connection from a known TOR node, the connection is blocked either with no further notice or with an error message or explanation is given. Some servers deploy additional authentication, such as solving Captchas, sending identification e-mail or requesting mobile phone authentication.

Countermeasures: The user may switch to a different form of anonymizer, which, however, may offer less protection than TOR. Alternatively, the user may choose to punish the provider by changing the supplier, or punishing the supplier by intentionally reverting to paper-based business transactions. Some users may abstain from buying products or services from blocking vendors and may use a public library instead.

Examples/Known Uses: In Figure 5, a selection of service providers that, during the past years, have deployed the pattern are listed.

Related Patterns: -

Psychological Aspects: The application of this pattern is caused in the exercise of power in a relationship. The psychological consequences are equal to those of being denied access to a social arena by a door bouncer.

Strategies: DENY, MAXIMIZE.

3 Conclusion

This article shows, from empirical evidence, how the dark patterns *Fogging identification with security*, *Sweet Seduction*, and *You can run but you can't hide* are being deployed in real-life situations to collect additional identity attributes from users of on-line services.

A specification of the dark patterns was provided, including their context and providing possible countermeasures on behalf of the user. In particular the wide-spread de-anonymization efforts of Internet identities over a span of several years looks noteworthy.

Ethical concerns are risen by the deployment of nudging techniques to collect additional identity attributes by deploying social group pressure, or by claiming higher goals, such as security, as the reasons for advanced data collection.

4 References

- [GD16s] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR). Official Journal of the European Union, 2016.
- [Aq12] Acquisti, A.: Nudging privacy: The behavioral economics of personal information. 2012.
- [Bö16] Bösch, C.; et al.: Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns. 2016.
- [Cl05] Clarke, R.: A sufficiently rich model of (id) entity, authentication and authorisation. London School of Economics LSE, London, 2009.
- [CHH16] Colesky, M.; Hoepman, J. H.; Hillen, C.: A Critical Analysis of Privacy Design Strategies. San Jose, USA, 2016.
- [DMS04] Dingledine, R.; Mathewson, N.; Syverson, P.: Tor: The second-generation onion router. DTIC Document, 2004.
- [DG13] Doty, N.; Gupta, M.: Privacy Design Patterns and Anti-Patterns. Trustbusters Workshop at the Symposium on Usable Privacy and Security, Newcastle, UK, 2013.
- [Fr07] Fritsch, L.: State of the Art of Privacy-enhancing Technology (PET) - Deliverable D.2.1 of the PET Web project. Norsk Regnesentral, Oslo, Norway, 2007.
- [Ho14] Hoepman, J.-H.: Privacy Design Strategies. Springer Berlin Heidelberg, 2014.
- [LFH17] Lenhard, J.; Fritsch, L.; Herold, S.: A Literature Study on Privacy Patterns Research. Euromicro Conference on Software Engineering and Advanced Applications (SEAA 2017), Vienna, IEEE Computer Society, 2017.
- [PF11] Painsil, E.; Fritsch, L.: A Taxonomy of Privacy and Security Risks Contributing Factors. Privacy and Identity Management for Life, Springer Boston, 2011.
- [PH10] Pfitzmann, A.; Hansen, M.: Anonymity, unlinkability, unobservability, pseudonymity, and identity management-a consolidated proposal for terminology. Technische Universität Dresden, Dresden, 2010.
- [Ro12] Roßnagel, H.; et al.: Futureid-shaping the future of electronic identity. 2012.

