EXAMINING THE INTERPLAY BETWEEN PRIVACY BY DESIGN (PBD) SCHEMES AND PRIVACY PATTERNS

Lamya Alkhariji
School of Computer Science and Informatics
Cardiff University, UK
AlkharijiLA@cardiff.ac.uk

Omer Rana
School of Computer Science and Informatics
Cardiff University, UK
RanaOF@cardiff.ac.uk

Charith Perera
School of Computer Science and Informatics
Cardiff University, UK
PereraC@cardiff.ac.uk

July 29, 2020

ABSTRACT

Privacy is a vague concept. This vagueness makes it difficult to understand what it means. Software engineering is an area such ambiguity creates a significant problem. For example, if the software developers do not understand privacy properly, they are not going to develop the software in a privacy-protected manner. To address this issue, as a community, over the last two decades, many researchers have proposed a few different Privacy by Design (PbD) schemes. Typically, PbD schemes comprise a set of instructions. These instructions are also referred to as guidelines, principles, strategies. Another way to address this problem of ambiguity is privacy patterns. Inspired by design patterns in software engineering domain, researchers and privacy experts have developed privacy patterns. Each Privacy pattern is designed to improve privacy in particular application design by eliminating certain privacy risks in a certain way. For our analysis, we identified ten (10) different PhD schemes. We analyse them against 74 different privacy patterns (`privacypatterns.eu`, `privacypatterns.org`). In this report, we examine the interplay between Privacy by Design (PbD) schemes and privacy patterns. This document contains the raw outcome of our analysis. Please refer to our research paper to read about insights we generated through this analysis.

Table 1: Privacy Schemes use in the Analysis

Citation	Type	Number
(1) Perera et al. [1]	Guidelines	30
(2) Hoepman [2]	Strategies	8
(3) Cavoukian [3]	Principles	7
(4) Cavoukian and Jonas [4]	Principles	7
(5) ISO 29100 Privacy framework [5]	Principles	11
(6) Wright and Raab [6]	Principles	9
(7) Fair Information Practice Principles (FIPPs) [7]	Principles	5
(8) Economic Cooperation and Development (OECD) [8]	Guidelines	8
(9) Rost and Bock [9]	Goals	6
(10) Fisk et al. [10]	Principles	3

***K*eywords** Privacy, Privacy by Design, Internet of Things, Privacy Knowledge Engineering

1 PbD Guidelines by Perera et al. [1]

Perera et al. [1] have proposed 30 privacy guidelines: (1) Minimise data acquisition, (2) Minimise number of data sources, (3) Minimise raw data intake, (4) Minimise knowledge discovery, (5) Minimise data storage, (6) Minimise data retention period, (7) Hidden data routing, (8) Data anonymisation, (9) Encrypted data communication, (10) Encrypted data processing, (11) Encrypted data storage, (12) Reduce data granularity, (13) . Query answering, (14) Repeated query blocking, (15) Distributed data storage, (16) Distributed data storage, (17) Knowledge discovery based aggregation, (18) Geography based aggregation, (19) Chain aggregation, (20) Time-Period based aggregation, (21) Category based aggregation, (22) Information Disclosure, (23) Control, (24) Logging, (25) Auditing, (26) Open Source, (27) Data Flow, (28) Certification, (29) Standardisation, (30) Compliance. More details can be found in [1].

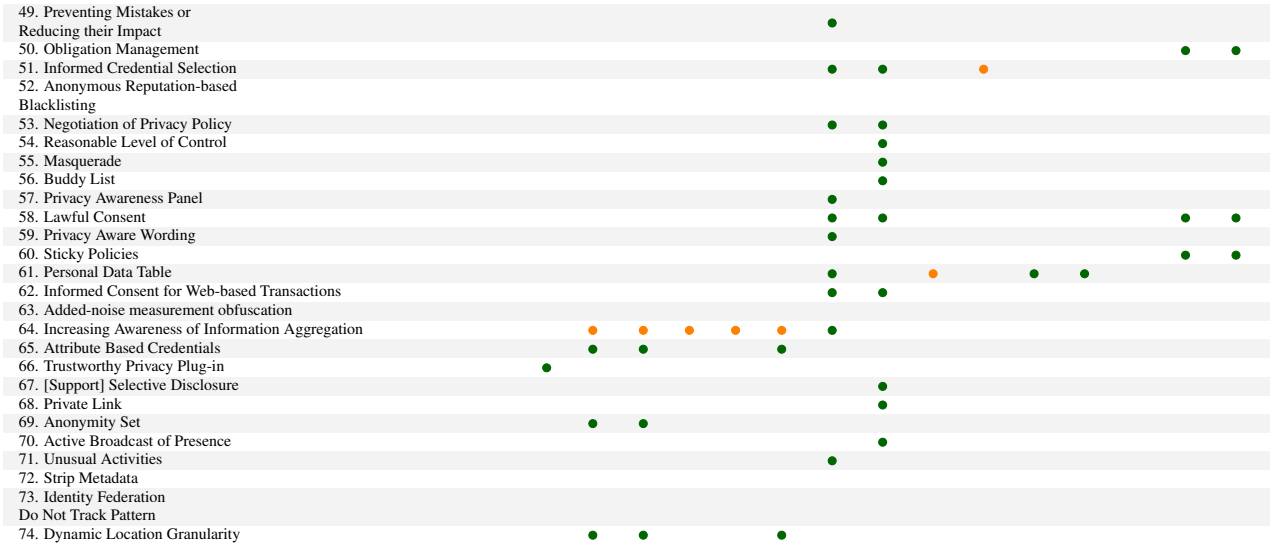
Table 2: Privacy Patterns Examined Against Privacy Strategies [1]

Privacy Pattern List	1. Minimise data acquisition	2. Minimise number of data sources	3. Minimise raw data intake	4. Minimise knowledge discovery	5. Minimise data storage	6. Minimise data retention period	7. Hidden data routing	8. Data anonymisation	9. Encrypted data communication	10. Encrypted data processing	11. Encrypted data storage	12. Reduce data granularity	13. Query answering	14. Repeated query	15. Distributed data processing
1. Protection against Tracking	●				●	●		●							
2. Location Granularity	●											●			
3. Minimal Information Asymmetry	●	○										○			
4. Informed Secure Passwords															
5. Awareness Feed.															
6. Encryption with user-managed keys	●										●				
7. Federated Privacy Impact Assessment															
8. Use of dummies				●											
9. Who's Listening															
10. Privacy Policy Display															
11. Layered Policy Design															
12. Discouraging Blanket Strategies												○			
13. Reciprocity															
14. Asynchronous notice															
15. Abridged Terms and Condition															
16. Policy Matching Display															
17. Incentivized Participation															
18. Outsourcing [with consent]															
19. Ambient Notice															
20. Dynamic Privacy Policy Display															
21. Privacy Labels															
22. Data Breach Notification Pattern															
23. Pseudonymous Messaging				●			●	○							
24. Onion Routing									●	●					
25. Strip Invisible Metadata	●			○											
26. Pseudonymous Identity								●					○		
27. Personal Data Store															
28. Trust Evaluation of Services Slides															
29. Aggregation Gateway									●	●	○			○	
30. Privacy icons															
31. Privacy-Aware Network Client															
32. Sign an Agreement															
33. Single Point of Contact															
34. Informed Implicit Consent															
35. Enable/Disable Function															
36. Privacy Color Coding															
37. Appropriate Privacy Icons															
38. User Data Confinement Pattern	●			○	●										●
39. Icons for Privacy Policies															
40. Obtaining Explicit Consent															
41. Privacy Mirrors															
42. Appropriate Privacy Feedback															
43. Impactful Information and Feedback															
44. Decoupling [content] and Location Information Visibility	●														
45. Platform for Privacy Preferences															
46. Selective Access control															
47. Pay Back															
48. Privacy Dashboard															
49. Preventing Mistakes or Reducing their Impact															
50. Obligation Management															
51. Informed Credential Selection															
52. Anonymous Reputation-based Blacklisting															
53. Negotiation of Privacy Policy															
54. Reasonable Level of Control															
55. Masquerade															

56. Buddy List																					
57. Privacy Awareness Panel																					
58. Lawful Consent																					
59. Privacy Aware Wording																					
60. Sticky Policies																					
61. Personal Data Table																					
62. Informed Consent for Web-based Transactions																					
63. Added-noise measurement obfuscation				●																	
64. Increasing Awareness of Information Aggregation																					
65. Attribute Based Credentials	●		●																		
66. Trustworthy Privacy Plug-in	●	●			●											●				●	
67. [Support] Selective Disclosure																					
68. Private Link																					
69. Anonymity Set				●				●								●					
70. Active Broadcast of Presence																					
71. Unusual Activities																					
72. Strip Metadata	●		●	●	●																
73. Identity Federation																					
Do Not Track Pattern																					
74. Dynamic Location Granularity	●															●					

Table 3: Privacy Patterns Examined Against Privacy Guidelines (continue) [1]

Privacy Pattern List	16. Distributed data storage	17. Knowledge discovery based aggregation	18. Geography based aggregation	19. Chain aggregation	20. Time-Period based aggregation	21. Category based aggregation	22. Information Disclosure	23. Control	24. Logging	25. Auditing	26. Open Source	27. Data Flow Data	28. Certification	29. Standardisation	30. Compliance
1. Protection against Tracking							●	●							
2. Location Granularity		●	●			●									
3. Minimal Information Asymmetry							●				●	●			
4. Informed Secure Passwords							●								
5. Awareness Feed.							●				●	●			
6. Encryption with user-managed keys								●							
7. Federated Privacy Impact Assessment															●
8. Use of dummies		●													
9. Who's Listening							●		●		●	●			
10. Privacy Policy Display							●		●		●	●		●	
11. Layered Policy Design							●		●		●	●		●	
12. Discouraging Blanket Strategies								●							
13. Reciprocity								●							
14. Asynchronous notice							●								●
15. Abridged Terms and Condition							●				●	●		●	
16. Policy Matching Display							●				●	●		●	
17. Incentivized Participation								●							
18. Outsourcing [with consent]															●
19. Ambient Notice							●								●
20. Dynamic Privacy Policy Display							●				●	●		●	
21. Privacy Labels							●				●	●		●	
22. Data Breach Notification Pattern							●		●	●					●
23. Pseudonymous Messaging															
24. Onion Routing															
25. Strip Invisible Metadata															
26. Pseudonymous Identity															
27. Personal Data Store							●	●							
28. Trust Evaluation of Services Slides													●	●	
29. Aggregation Gateway		●													
30. Privacy icons							●				●	●		●	
31. Privacy-Aware Network Client							●				●	●			
32. Sign an Agreement														●	●
33. Single Point of Contact	●							●							
34. Informed Implicit Consent							●								●
35. Enable/Disable Function								●							
36. Privacy Color Coding							●				●	●		●	
37. Appropriate Privacy Icons							●				●	●		●	
38. User Data Confinement Pattern	●							●							
39. Icons for Privacy Policies							●				●	●		●	
40. Obtaining Explicit Consent							●								●
41. Privacy Mirrors							●				●	●			
42. Appropriate Privacy Feedback							●				●	●			
43. Impactful Information and Feedback							●				●	●			
44. Decoupling [content] and Location Information Visibility								●							
45. Platform for Privacy Preferences							●								
46. Selective Access control								●							
47. Pay Back								●							
48. Privacy Dashboard							●	●	●	●					

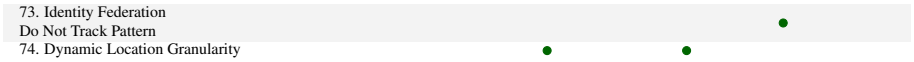

49. Preventing Mistakes or Reducing their Impact
50. Obligation Management
51. Informed Credential Selection
52. Anonymous Reputation-based Blacklisting
53. Negotiation of Privacy Policy
54. Reasonable Level of Control
55. Masquerade
56. Buddy List
57. Privacy Awareness Panel
58. Lawful Consent
59. Privacy Aware Wording
60. Sticky Policies
61. Personal Data Table
62. Informed Consent for Web-based Transactions
63. Added-noise measurement obfuscation
64. Increasing Awareness of Information Aggregation
65. Attribute Based Credentials
66. Trustworthy Privacy Plug-in
67. [Support] Selective Disclosure
68. Private Link
69. Anonymity Set
70. Active Broadcast of Presence
71. Unusual Activities
72. Strip Metadata
73. Identity Federation Do Not Track Pattern
74. Dynamic Location Granularity

2 PbD Strategies by Hoepman et al. [2]

Hoepman et al. [2] have proposed eight privacy strategies: (1) Minimise, (2) Hide, (3) Separate, (4) Aggregate, (5) Inform, (6) Control, (7) Enforce, (8) Demonstrate. More details can be found in [2].

Table 4: Privacy Patterns Examined Against Privacy Strategies [2]

Privacy Pattern List	1. Minimize	2. Hide	3. Separate	4. Aggregate	5. Inform	6. Control	7. Enforce	8. Demonstrate
1. Protection against Tracking	●			○		●		
2. Location Granularity	●	○				●		
3. Minimal Information Asymmetry					●		○	
4. Informed Secure Passwords					●		○	
5. Awareness Feed.					●			
6. Encryption with user-managed keys		●				○		
7. Federated Privacy Impact Assessment							●	●
8. Use of dummies		○		○				
9. Who's Listening					●			
10. Privacy Policy Display					●			●
11. Layered Policy Design					●			●
12. Discouraging Blanket Strategies		○				●		
13. Reciprocity				○	●			
14. Asynchronous notice					●			
15. Abridged Terms and Condition					●			●
16. Policy Matching Display					●			●
17. Incentivized Participation								
18. Outsourcing [with consent]						●		
19. Ambient Notice					●			
20. Dynamic Privacy Policy Display					●			●
21. Privacy Labels					●			○
22. Data Breach Notification Pattern					●			○
23. Pseudonymous Messaging		●						
24. Onion Routing		●						
25. Strip Invisible Metadata	●	○						
26. Pseudonymous Identity	●			●		○		
27. Personal Data Store					●			●
28. Trust Evaluation of Services Slides					●			●
29. Aggregation Gateway		●	●	●				
30. Privacy icons					●			●
31. Privacy-Aware Network Client					●			●
32. Sign an Agreement					●	●		
33. Single Point of Contact						●		
34. Informed Implicit Consent					●			
35. Enable/Disable Function						●		
36. Privacy Color Coding					●			●
37. Appropriate Privacy Icons					●			●
38. User Data Confinement Pattern	○		●					
39. Icons for Privacy Policies					●			●
40. Obtaining Explicit Consent						●		
41. Privacy Mirrors					●			
42. Appropriate Privacy Feedback					●			●
43. Impactful Information and Feedback					●			●
44. Decoupling [content] and Location Information Visibility	○					●		
45. Platform for Privacy Preferences					●	●		
46. Selective Access control						●		
47. Pay Back								
48. Privacy Dashboard					●	●		●
49. Preventing Mistakes or Reducing their Impact					●			●
50. Obligation Management							●	
51. Informed Credential Selection					●			●
52. Anonymous Reputation-based Blacklisting			●	●				
53. Negotiation of Privacy Policy					●			
54. Reasonable Level of Control						●		
55. Masquerade				●		●		
56. Buddy List						●		
57. Privacy Awareness Panel					●			●
58. Lawful Consent						●		●
59. Privacy Aware Wording					●			●
60. Sticky Policies							●	
61. Personal Data Table					●			●
62. Informed Consent for Web-based Transactions					●	●		
63. Added-noise measurement obfuscation	●	●						
64. Increasing Awareness of Information Aggregation					●			
65. Attribute Based Credentials	●	○		●				
66. Trustworthy Privacy Plug-in		●		●		●		
67. [Support] Selective Disclosure						●		
68. Private Link						●		
69. Anonymity Set		●		●				
70. Active Broadcast of Presence						●		
71. Unusual Activities					●			
72. Strip Metadata	●	●						


73. Identity Federation
Do Not Track Pattern
74. Dynamic Location Granularity

3 PbD Principles by Cavoukian et al. [3]

Cavoukian [3] has proposed seven Privacy by Design foundation principles: (1) Proactive not Reactive; Preventative not Remedial, (2) Privacy as the Default Setting, (3) Privacy Embedded into Design, (4) Full Functionality-Positive - Sum, not Zero-Sum, (5) End-to-End Security - Full Lifecycle Protection, (6) Visibility and Transparency - Keep it Open, (7) Respect for User Privacy - Keep it User-Centric. Detailed are presented in [3].

Table 5: Privacy Patterns Examined Against Privacy Strategies [2]

Privacy Pattern List	1. Proactive not Reactive; Preventative not Remedial	2. Privacy as the Default Setting	3. Privacy Embedded into Design	4. Full Functionality-Positive-Sum, not Zero-Sum	5. End-to-End Security-Full Lifecycle Protection	6. Visibility and Transparency-Keep it Open	7. Respect for User Privacy-Keep it User-Centric
1. Protection against Tracking	●	●	●				●
2. Location Granularity	●	●	●				●
3. Minimal Information Asymmetry	●	●	●			●	●
4. Informed Secure Passwords	●		●		●		●
5. Awareness Feed.	●		●			●	●
6. Encryption with user-managed keys	●	●	●		●		
7. Federated Privacy Impact Assessment	●		●				
8. Use of dummies	●	●	●				
9. Who's Listening	●					●	●
10. Privacy Policy Display						●	
11. Layered Policy Design						●	
12. Discouraging Blanket Strategies	●		●				●
13. Reciprocity			●				●
14. Asynchronous notice						●	
15. Abridged Terms and Condition						●	
16. Policy Matching Display						●	●
17. Incentivized Participation			●				●
18. Outsourcing [with consent]	●		●			●	
19. Ambient Notice	●		●			●	●
20. Dynamic Privacy Policy Display	●					●	
21. Privacy Labels						●	
22. Data Breach Notification Pattern						●	●
23. Pseudonymous Messaging	●	●	●		●		
24. Onion Routing	●	●	●		●		
25. Strip Invisible Metadata	●	●	●				
26. Pseudonymous Identity	●	●	●	●			
27. Personal Data Store	●		●			●	●
28. Trust Evaluation of Services Slides						●	
29. Aggregation Gateway	●		●		●		
30. Privacy icons						●	
31. Privacy-Aware Network Client						●	
32. Sign an Agreement	●					●	●
33. Single Point of Contact	●		●		●		●
34. Informed Implicit Consent						●	●
35. Enable/Disable Function			●				●
36. Privacy Color Coding						●	
37. Appropriate Privacy Icons						●	
38. User Data Confinement Pattern	●	●	●				
39. Icons for Privacy Policies						●	
40. Obtaining Explicit Consent						●	●
41. Privacy Mirrors						●	●
42. Appropriate Privacy Feedback						●	●
43. Impactful Information and Feedback						●	●
44. Decoupling [content] and Location Information Visibility	●	●	●				●
45. Platform for Privacy Preferences			●				●
46. Selective Access control	●		●				●
47. Pay Back			●				●
48. Privacy Dashboard			●			●	●
49. Preventing Mistakes or Reducing their Impact						●	●
50. Obligation Management		●	●				
51. Informed Credential Selection						●	●
52. Anonymous Reputation-based Blacklisting	●		●		●		
53. Negotiation of Privacy Policy			●				●
54. Reasonable Level of Control	●		●				●
55. Masquerade			●		●		
56. Buddy List			●				●

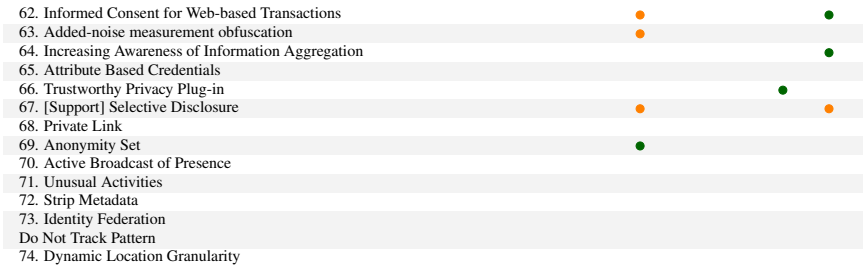
57. Privacy Awareness Panel			●	●	
58. Lawful Consent	●			●	●
59. Privacy Aware Wording				●	
60. Sticky Policies	●	●	●		
61. Personal Data Table			●	●	
62. Informed Consent for Web-based Transactions		●		●	●
63. Added-noise measurement obfuscation	●	●	●		
64. Increasing Awareness of Information Aggregation				●	●
65. Attribute Based Credentials	●	●			
66. Trustworthy Privacy Plug-in	●	●	●		
67. [Support] Selective Disclosure					●
68. Private Link			●		●
69. Anonymity Set	●	●			
70. Active Broadcast of Presence			●		●
71. Unusual Activities			●		●
72. Strip Metadata	●	●			
73. Identity Federation					
Do Not Track Pattern					
74. Dynamic Location Granularity		●	●		

4 PbD Principles by Cavoukian and Jonas [4]

Cavoukian and Jonas [4] has proposed seven privacy principles by extending the Cavoukian's privacy principle [] as follows: (1) Full Attribution, (2) Data Tethering, (3) Analytics on Anonymised Data, (4) Tamper-Resistant Audit Logs, (5) False Negative Favouring Methods, (6) Self-Correcting False Positives, (7) Information Transfer Accounting. More details can be found in [].

Table 6: Privacy Patterns Examined Against Privacy Strategies [2]

Privacy Pattern List	1. Full Attribution	2. Data Tethering	3. Analytics on Anonymised Data	4. Tamper-Resistant Audit Logs	5. False Negative Favouring Methods	6. Self-Correcting False Positives	7. Information Transfer Accounting
1. Protection against Tracking			●				
2. Location Granularity							
3. Minimal Information Asymmetry							
4. Informed Secure Passwords							
5. Awareness Feed.			●				●
6. Encryption with user-managed keys				●			
7. Federated Privacy Impact Assessment			●				
8. Use of dummies							
9. Who's Listening							
10. Privacy Policy Display							
11. Layered Policy Design							
12. Discouraging Blanket Strategies							
13. Reciprocity							
14. Asynchronous notice							
15. Abridged Terms and Condition							
16. Policy Matching Display							
17. Incentivized Participation							
18. Outsourcing [with consent]							
19. Ambient Notice							
20. Dynamic Privacy Policy Display							
21. Privacy Labels							
22. Data Breach Notification Pattern	●	●					
23. Pseudonymous Messaging			●				
24. Onion Routing			●				
25. Strip Invisible Metadata							
26. Pseudonymous Identity			●				
27. Personal Data Store	●	●				●	
28. Trust Evaluation of Services Slides				●			●
29. Aggregation Gateway			●	●			●
30. Privacy icons				●			
31. Privacy-Aware Network Client							
32. Sign an Agreement							
33. Single Point of Contact							
34. Informed Implicit Consent							
35. Enable/Disable Function							
36. Privacy Color Coding							
37. Appropriate Privacy Icons							
38. User Data Confinement Pattern			●	●			
39. Icons for Privacy Policies							
40. Obtaining Explicit Consent							●
41. Privacy Mirrors	●	●		●		●	●
42. Appropriate Privacy Feedback							
43. Impactful Information and Feedback							
44. Decoupling [content] and Location Information Visibility							
45. Platform for Privacy Preferences							
46. Selective Access control							●
47. Pay Back							
48. Privacy Dashboard						●	
49. Preventing Mistakes or Reducing their Impact					●	●	●
50. Obligation Management	●		●				●
51. Informed Credential Selection			●	●			●
52. Anonymous Reputation-based Blacklisting							
53. Negotiation of Privacy Policy			●				
54. Reasonable Level of Control			●			●	
55. Masquerade			●				
56. Buddy List							
57. Privacy Awareness Panel							●
58. Lawful Consent							
59. Privacy Aware Wording							●
60. Sticky Policies							
61. Personal Data Table						●	

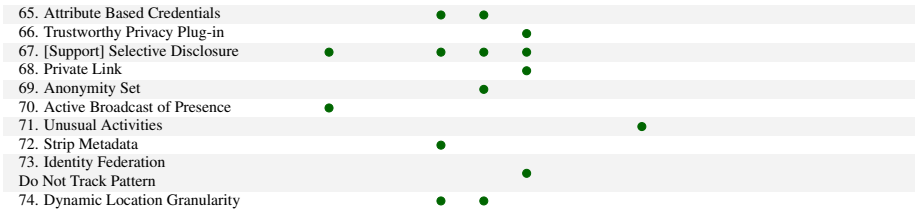

62. Informed Consent for Web-based Transactions
63. Added-noise measurement obfuscation
64. Increasing Awareness of Information Aggregation
65. Attribute Based Credentials
66. Trustworthy Privacy Plug-in
67. [Support] Selective Disclosure
68. Private Link
69. Anonymity Set
70. Active Broadcast of Presence
71. Unusual Activities
72. Strip Metadata
73. Identity Federation
Do Not Track Pattern
74. Dynamic Location Granularity

5 PbD Principles by ISO 29100 Privacy framework [5]

ISO 29100 [5] has proposed 11 privacy principles: (1) Consent and choice, (2)Purpose legitimacy and specification, (3) Collection limitation, (4). Data minimisation, (5) Use, retention and disclosure limitation,(6) Accuracy and quality, (7). Openness, transparency and notice, (8) Individual participation and access, (9) Accountability, (10) Information security, (11) Privacy compliance. Detailed can be found in [5]

Table 7: Privacy Patterns Examined Against Privacy Principles [5]

Privacy Pattern List	1. Consent and choice	2. Purpose legitimacy and specification	3. Collection limitation	4. Data minimization	5. Use,retention and disclosure limitation	6. Accuracy and quality	7. Openness, transparency and notice	8. Individual participation and access	09. Accountability	10. Information security	11. Privacy compliance
1. Protection against Tracking			●	●	●						
2. Location Granularity	●	●	●	●	●						
3. Minimal Information Asymmetry	●	●	●	●	●		●				
4. Informed Secure Passwords										●	
5. Awareness Feed.							●				
6. Encryption with user-managed keys	●				●			●		●	
7. Federated Privacy Impact Assessment				●							●
8. Use of dummies				●							
9. Who's Listening							●	●			
10. Privacy Policy Display							●		●		
11. Layered Policy Design							●		●		
12. Discouraging Blanket Strategies	●			●	●		●	●			
13. Reciprocity				●	●						
14. Asynchronous notice		●					●		●		
15. Abridged Terms and Condition		●					●		●		
16. Policy Matching Display		●					●		●		
17. Incentivized Participation								●			
18. Outsourcing [with consent]	●			●	●		●	●	●		
19. Ambient Notice							●	●			
20. Dynamic Privacy Policy Display		●					●		●		
21. Privacy Labels		●					●		●		
22. Data Breach Notification Pattern						●	●		●		
23. Pseudonymous Messaging				●	●						
24. Onion Routing				●	●					●	
25. Strip Invisible Metadata			●	●							
26. Pseudonymous Identity				●	●					●	
27. Personal Data Store	●			●	●	●	●	●			
28. Trust Evaluation of Services Slides							●		●		
29. Aggregation Gateway				●	●				●	●	
30. Privacy icons		●					●		●		
31. Privacy-Aware Network Client		●					●		●		
32. Sign an Agreement to Solve Lack of Trust on the Use of Private Data Context	●						●		●		●
33. Single Point of Contact					●	●	●	●		●	
34. Informed Implicit Consent	●						●				
35. Enable/Disable Function	●		●	●	●						
36. Privacy Color Coding		●					●		●		
37. Appropriate Privacy Icons		●					●		●		
38. User Data Confinement Pattern			●	●	●			●		●	
39. Icons for Privacy Policies		●					●		●		
40. Obtaining Explicit Consent	●						●		●		
41. Privacy Mirrors						●	●	●			
42. Appropriate Privacy Feedback							●		●		
43. Impactful Information and Feedback							●		●		
44. Decoupling [content] and Location Information Visibility	●		●	●	●			●			
45. Platform for Privacy Preferences	●					●			●		
46. Selective Access control	●			●	●			●			
47. Pay Back											
48. Privacy Dashboard	●				●	●	●	●			
49. Preventing Mistakes or Reducing their Impact						●	●		●		●
50. Obligation Management					●	●			●		●
51. Informed Credential Selection	●						●		●		●
52. Anonymous Reputation-based Blacklisting									●	●	●
53. Negotiation of Privacy Policy	●						●			●	●
54. Reasonable Level of Control	●	●	●	●							
55. Masquerade	●		●	●							
56. Buddy List	●			●	●						
57. Privacy Awareness Panel					●	●	●	●	●		
58. Lawful Consent	●	●					●		●		●
59. Privacy Aware Wording		●					●		●		
60. Sticky Policies	●				●	●	●	●	●		●
61. Personal Data Table	●						●	●			
62. Informed Consent for Web-based Transactions	●						●		●		
63. Added-noise measurement obfuscation				●	●						
64. Increasing Awareness of Information Aggregation							●		●		

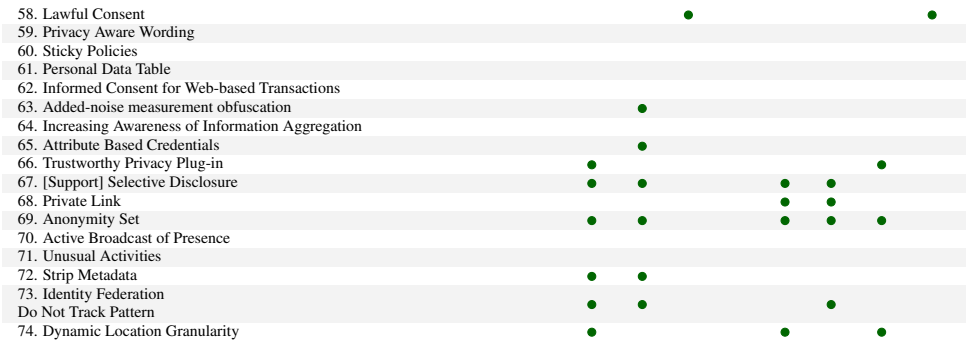

65. Attribute Based Credentials
66. Trustworthy Privacy Plug-in
67. [Support] Selective Disclosure
68. Private Link
69. Anonymity Set
70. Active Broadcast of Presence
71. Unusual Activities
72. Strip Metadata
73. Identity Federation
Do Not Track Pattern
74. Dynamic Location Granularity

6 PbD Principles by Wright and Raab [6]

Wright and Raab [6] Privacy Principles have proposed nine privacy principles (1) Right to dignity, (2) Right to be let alone, (3) Right to anonymity, (4) Right to autonomy, (5) . Right to individuality and uniqueness of identity, (6) Right to assemble or associate with others without being surveilled, (7) Right to confidentiality and secrecy of communications, (8) Right to travel (in physical or cyber space) without being tracked, (9) People should not have to pay in order to exercise their rights of privacy (subject to any justifiable exceptions), nor be denied goods or services or offered them on a less preferential basis. Detailed are presented in [6].

Table 8: Privacy Patterns Examined Against Privacy Strategies [2]

Privacy Pattern List	1. Right to dignity	2. Right to be let alone	3. Right to anonymity	4. Right to autonomy	5. Right to individuality	6. Right to assemble	7. Right to confidentiality	8. Right to travel without being tracked	9. People should not have to pay
1. Protection against Tracking		●						●	
2. Location Granularity		●				●	●		
3. Minimal Information Asymmetry									
4. Informed Secure Passwords							●		
5. Awareness Feed.	●					●	●	●	
6. Encryption with user-managed keys		●					●		
7. Federated Privacy Impact Assessment							●		
8. Use of dummies		●	●					●	
9. Who's Listening	●								
10. Privacy Policy Display									
11. Layered Policy Design									
12. Discouraging Blanket Strategies	●	●					●		
13. Reciprocity									
14. Asynchronous notice	●	●				●	●	●	
15. Abridged Terms and Condition									
16. Policy Matching Display									
17. Incentivized Participation	●								
18. Outsourcing [with consent]	●	●							
19. Ambient Notice	●	●				●	●	●	
20. Dynamic Privacy Policy Display									
21. Privacy Labels									
22. Data Breach Notification Pattern							●		
23. Pseudonymous Messaging		●	●				●	●	
24. Onion Routing			●				●		
25. Strip Invisible Metadata		●						●	
26. Pseudonymous Identity		●	●						
27. Personal Data Store	●								
28. Trust Evaluation of Services Slides									
29. Aggregation Gateway		●							
30. Privacy icons									
31. Privacy-Aware Network Client									
32. Sign an Agreement									
33. Single Point of Contact									
34. Informed Implicit Consent	●					●		●	
35. Enable/Disable Function		●					●	●	
36. Privacy Color Coding									
37. Appropriate Privacy Icons									
38. User Data Confinement Pattern	●	●						●	
39. Icons for Privacy Policies									
40. Obtaining Explicit Consent	●						●	●	
41. Privacy Mirrors	●								
42. Appropriate Privacy Feedback		●				●		●	
43. Impactful Information and Feedback									
44. Decoupling [content] and Location Information Visibility		●				●		●	
45. Platform for Privacy Preferences		●					●		
46. Selective Access control							●		
47. Pay Back	●								
48. Privacy Dashboard									
49. Preventing Mistakes or Reducing their Impact	●				●				
50. Obligation Management									
51. Informed Credential Selection									
52. Anonymous Reputation-based Blacklisting	●		●						
53. Negotiation of Privacy Policy				●			●		
54. Reasonable Level of Control		●	●			●	●	●	
55. Masquerade	●	●	●			●	●		
56. Buddy List	●	●							
57. Privacy Awareness Panel									


58. Lawful Consent
59. Privacy Aware Wording
60. Sticky Policies
61. Personal Data Table
62. Informed Consent for Web-based Transactions
63. Added-noise measurement obfuscation
64. Increasing Awareness of Information Aggregation
65. Attribute Based Credentials
66. Trustworthy Privacy Plug-in
67. [Support] Selective Disclosure
68. Private Link
69. Anonymity Set
70. Active Broadcast of Presence
71. Unusual Activities
72. Strip Metadata
73. Identity Federation
Do Not Track Pattern
74. Dynamic Location Granularity

7 PbD Principles by Fair Information Practice Principles (FIPPs) [7]

Fair Information Practice Principles (FIPPs) [7] comprises of five privacy principles: (1) Notice / Awareness, (2) Choice / Consent Choice, (3) Access / Participation, (4) Integrity / Security, (5) Enforcement / Redress. Detailed are presented in [7].

Table 9: Privacy Patterns Examined Against Privacy Strategies [2]

Privacy Pattern List	1. Notice / Awareness	2. Choice / Consent Choice	3. Access / Participation	4. Integrity / Security	5. Enforcement / Redress
1. Protection against Tracking		●			
2. Location Granularity					
3. Minimal Information Asymmetry	●				
4. Informed Secure Passwords	●			●	
5. Awareness Feed.	●				
6. Encryption with user-managed keys			●	○	
7. Federated Privacy Impact Assessment					●
8. Use of dummies				○	
9. Who's Listening	●				
10. Privacy Policy Display	●				
11. Layered Policy Design	●				
12. Discouraging Blanket Strategies		●			
13. Reciprocity					
14. Asynchronous notice	●				
15. Abridged Terms and Condition	●				
16. Policy Matching Display	●				
17. Incentivized Participation					
18. Outsourcing [with consent]	○				
19. Ambient Notice	●				
20. Dynamic Privacy Policy Display	●				
21. Privacy Labels	●				
22. Data Breach Notification Pattern	●			○	
23. Pseudonymous Messaging				○	
24. Onion Routing				●	
25. Strip Invisible Metadata					
26. Pseudonymous Identity		○			
27. Personal Data Store			●		
28. Trust Evaluation of Services Slides					
29. Aggregation Gateway				●	
30. Privacy icons	●				
31. Privacy-Aware Network Client	●				
32. Sign an Agreement	●	●			
33. Single Point of Contact		●		●	
34. Informed Implicit Consent	●	○			
35. Enable/Disable Function		●			
36. Privacy Color Coding	●				
37. Appropriate Privacy Icons	●				
38. User Data Confinement Pattern				●	
39. Icons for Privacy Policies	●				
40. Obtaining Explicit Consent	●	●			
41. Privacy Mirrors	●		●		
42. Appropriate Privacy Feedback	●				
43. Impactful Information and Feedback	●				
44. Decoupling [content] and Location Information Visibility				○	
45. Platform for Privacy Preferences	●				
46. Selective Access control		●			
47. Pay Back					
48. Privacy Dashboard	●	●	●		
49. Preventing Mistakes or Reducing their Impact	●				
50. Obligation Management					
51. Informed Credential Selection	●				
52. Anonymous Reputation-based Blacklisting					
53. Negotiation of Privacy Policy	●				
54. Reasonable Level of Control		●			
55. Masquerade		●			
56. Buddy List		●			
57. Privacy Awareness Panel	●				
58. Lawful Consent		●			
59. Privacy Aware Wording	●				
60. Sticky Policies					
61. Personal Data Table	●		○		
62. Informed Consent for Web-based Transactions	●	●			
63. Added-noise measurement obfuscation				●	
64. Increasing Awareness of Information Aggregation	●				
65. Attribute Based Credentials				○	
66. Trustworthy Privacy Plug-in					


67. [Support] Selective Disclosure
68. Private Link
69. Anonymity Set
70. Active Broadcast of Presence
71. Unusual Activities
72. Strip Metadata
73. Identity Federation
Do Not Track Pattern
74. Dynamic Location Granularity

8 PbD Guidelines by (OECD) Oleary 1995 [8]

There are eight OECD Personal Privacy Guidelines, namely, (1) Collection limitation, (2) Data quality, (3) Purpose specification, (4) Use limitation, (5) Security safeguards, (6) Openness, (7) Individual participation, (8) Accountability. More details can be found in [8].

Table 10: Privacy Patterns Examined Against Privacy Strategies [2]

Privacy Pattern List	1. Collection limitation	2. Data quality	3. Purpose specification	4. Use limitation	5. Security safeguards	6. Openness	7. Individual participation	8. Accountability
1. Protection against Tracking	●						●	
2. Location Granularity	●		●					
3. Minimal Information Asymmetry						●		
4. Informed Secure Passwords					●			
5. Awareness Feed.						●		
6. Encryption with user-managed keys					●		●	
7. Federated Privacy Impact Assessment								●
8. Use of dummies					●			
9. Who's Listening						●		
10. Privacy Policy Display						●		
11. Layered Policy Design						●		
12. Discouraging Blanket Strategies							●	
13. Reciprocity							●	
14. Asynchronous notice						●		
15. Abridged Terms and Condition						●		
16. Policy Matching Display						●		
17. Incentivized Participation							●	
18. Outsourcing [with consent]				●			●	●
19. Ambient Notice						●		
20. Dynamic Privacy Policy Display						●		
21. Privacy Labels						●		
22. Data Breach Notification Pattern					●	●		
23. Pseudonymous Messaging	●			●	●			
24. Onion Routing					●			
25. Strip Invisible Metadata	●							
26. Pseudonymous Identity	●						●	
27. Personal Data Store		●					●	
28. Trust Evaluation of Services Slides						●		
29. Aggregation Gateway				●	●			
30. Privacy icons						●		
31. Privacy-Aware Network Client						●		
32. Sign an Agreement						●	●	
33. Single Point of Contact							●	
34. Informed Implicit Consent						●		
35. Enable/Disable Function							●	
36. Privacy Color Coding						●		
37. Appropriate Privacy Icons						●		
38. User Data Confinement Pattern	●			●				
39. Icons for Privacy Policies						●		
40. Obtaining Explicit Consent						●	●	
41. Privacy Mirrors						●		
42. Appropriate Privacy Feedback						●		
43. Impactful Information and Feedback						●		
44. Decoupling [content] and Location Information Visibility	●						●	
45. Platform for Privacy Preferences						●	●	
46. Selective Access control							●	
47. Pay Back							●	
48. Privacy Dashboard		●				●	●	
49. Preventing Mistakes or Reducing their Impact						●		●
50. Obligation Management								●
51. Informed Credential Selection						●		
52. Anonymous Reputation-based Blacklisting					●			
53. Negotiation of Privacy Policy						●	●	
54. Reasonable Level of Control							●	
55. Masquerade	●						●	
56. Buddy List							●	
57. Privacy Awareness Panel						●		
58. Lawful Consent							●	
59. Privacy Aware Wording						●		
60. Sticky Policies								●
61. Personal Data Table						●		
62. Informed Consent for Web-based Transactions						●	●	
63. Added-noise measurement obfuscation					●			
64. Increasing Awareness of Information Aggregation						●		
65. Attribute Based Credentials	●							
66. Trustworthy Privacy Plug-in							●	


67. [Support] Selective Disclosure
68. Private Link
69. Anonymity Set
70. Active Broadcast of Presence
71. Unusual Activities
72. Strip Metadata
73. Identity Federation
Do Not Track Pattern
74. Dynamic Location Granularity

9 PbD Goals by Rost and Bock [9]

Rost and Bock [9] have proposed six privacy goals: (1) Availability, (2) Integrity, (3) Confidentiality, (4) Transparency, (5) Unlinkability, (6) Ability to intervene. More details can be found in [9].

Table 11: Privacy Patterns Examined Against Privacy Strategies [2]

Privacy Pattern List	1. Availability	2. Integrity	3. Confidentiality	4. Transparency	5. Unlinkability	6. Ability to intervene
1. Protection against Tracking						●
2. Location Granularity						●
3. Minimal Information Asymmetry	●	◐			●	
4. Informed Secure Passwords						
5. Awareness Feed.		◐		◐		
6. Encryption with user-managed keys			●			◐
7. Federated Privacy Impact Assessment		●				
8. Use of dummies					●	
9. Who's Listening				●		
10. Privacy Policy Display				●		
11. Layered Policy Design				●		
12. Discouraging Blanket Strategies						●
13. Reciprocity						●
14. Asynchronous notice				●		
15. Abridged Terms and Condition				●		
16. Policy Matching Display				●		
17. Incentivized Participation						●
18. Outsourcing [with consent]				●		●
19. Ambient Notice				●		
20. Dynamic Privacy Policy Display				●		
21. Privacy Labels				●		
22. Data Breach Notification Pattern		◐		●		
23. Pseudonymous Messaging			●		●	
24. Onion Routing			●			
25. Strip Invisible Metadata						
26. Pseudonymous Identity					●	
27. Personal Data Store	●			●		●
28. Trust Evaluation of Services Slides						
29. Aggregation Gateway			◐		◐	
30. Privacy icons				●		
31. Privacy-Aware Network Client				●		
32. Sign an Agreement						●
33. Single Point of Contact						●
34. Informed Implicit Consent		◐		●		
35. Enable/Disable Function						●
36. Privacy Color Coding				●		
37. Appropriate Privacy Icons				●		
38. User Data Confinement Pattern					◐	
39. Icons for Privacy Policies				●		
40. Obtaining Explicit Consent				●		●
41. Privacy Mirrors	●			●		
42. Appropriate Privacy Feedback	●			●		
43. Impactful Information and Feedback				●		
44. Decoupling [content] and Location Information Visibility						●
45. Platform for Privacy Preferences				●		●
46. Selective Access control						●
47. Pay Back						●
48. Privacy Dashboard	●			●		●
49. Preventing Mistakes or Reducing their Impact				●		
50. Obligation Management		●				
51. Informed Credential Selection				●		
52. Anonymous Reputation-based Blacklisting						
53. Negotiation of Privacy Policy				●		●
54. Reasonable Level of Control						●
55. Masquerade						●
56. Buddy List						●
57. Privacy Awareness Panel	●			●		
58. Lawful Consent				●		●
59. Privacy Aware Wording				●		
60. Sticky Policies		●				
61. Personal Data Table	●			●		
62. Informed Consent for Web-based Transactions				●		●
63. Added-noise measurement obfuscation					●	
64. Increasing Awareness of Information Aggregation		◐			●	
65. Attribute Based Credentials					●	
66. Trustworthy Privacy Plug-in		◐	◐			
67. [Support] Selective Disclosure						●
68. Private Link						●
69. Anonymity Set					●	


70. Active Broadcast of Presence
71. Unusual Activities
72. Strip Metadata
73. Identity Federation
Do Not Track Pattern
74. Dynamic Location Granularity

10 PbD Principle by Fisk et al. [10]

Fisk et al. [10] have proposed three privacy principles: (1) Principle of Least Disclosure, (2) Principle of Qualitative Evaluation, (3) Principle of Forward Progress. More details can be found in [10].

Table 12: Privacy Patterns Examined Against Privacy Strategies [2]

Privacy Pattern List	1. Principle of Least Disclosure	2. Principle of Qualitative Evaluation	3. Principle of Forward Progress
1. Protection against Tracking	●	●	●
2. Location Granularity	●	●	●
3. Minimal Information Asymmetry			
4. Informed Secure Passwords			
5. Awareness Feed.			
6. Encryption with user-managed keys			
7. Federated Privacy Impact Assessment	●	●	●
8. Use of dummies	●		●
9. Who's Listening	●	●	●
10. Privacy Policy Display			
11. Layered Policy Design			
12. Discouraging Blanket Strategies	●	●	●
13. Reciprocity	●	●	●
14. Asynchronous notice			
15. Abridged Terms and Condition			
16. Policy Matching Display			
17. Incentivized Participation			
18. Outsourcing [with consent]	●	●	●
19. Ambient Notice			
20. Dynamic Privacy Policy Display			
21. Privacy Labels			
22. Data Breach Notification Pattern			
23. Pseudonymous Messaging	●		●
24. Onion Routing	●		●
25. Strip Invisible Metadata	●	●	●
26. Pseudonymous Identity	●	●	●
27. Personal Data Store		●	●
28. Trust Evaluation of Services Slides	●	●	●
29. Aggregation Gateway	●	●	●
30. Privacy icons			
31. Privacy-Aware Network Client			
32. Sign an Agreement			
33. Single Point of Contact			
34. Informed Implicit Consent			
35. Enable/Disable Function	●	●	●
36. Privacy Color Coding			
37. Appropriate Privacy Icons			
38. User Data Confinement Pattern	●	●	●
39. Icons for Privacy Policies			
40. Obtaining Explicit Consent			
41. Privacy Mirrors			
42. Appropriate Privacy Feedback			
43. Impactful Information and Feedback			
44. Decoupling [content] and Location Information Visibility	●	●	●
45. Platform for Privacy Preferences		●	●
46. Selective Access control	●	●	●
47. Pay Back	●	●	●
48. Privacy Dashboard			
49. Preventing Mistakes or Reducing their Impact	●	●	●
50. Obligation Management			
51. Informed Credential Selection	●	●	●
52. Anonymous Reputation-based Blacklisting			
53. Negotiation of Privacy Policy			
54. Reasonable Level of Control	●	●	●
55. Masquerade	●	●	●
56. Buddy List			
57. Privacy Awareness Panel			
58. Lawful Consent			
59. Privacy Aware Wording			
60. Sticky Policies			
61. Personal Data Table			
62. Informed Consent for Web-based Transactions			
63. Added-noise measurement obfuscation	●	●	●
64. Increasing Awareness of Information Aggregation			

65. Attribute Based Credentials	●	●	●
66. Trustworthy Privacy Plug-in			
67. [Support] Selective Disclosure	●	●	●
68. Private Link	●	●	●
69. Anonymity Set	●	●	●
70. Active Broadcast of Presence	●		●
71. Unusual Activities			
72. Strip Metadata	●	●	●
73. Identity Federation Do Not Track Pattern	●		
74. Dynamic Location Granularity	●	●	●

References

[1] Charith Perera, Mahmoud Barhamgi, Arosha K. Bandara, Muhammad Ajmal, Blaine Price, and Bashar Nuseibeh. Designing Privacy-aware Internet of Things Applications. *Information Sciences*, 512:238–257, mar 2020.

[2] Jaap-Henk Hoepman. Privacy Design Strategies. In Nora Cuppens-Boulahia, Frédéric Cuppens, Sushil Jajodia, Anas Abou El Kalam, and Thierry Sans, editors, *ICT Systems Security and Privacy Protection*, volume 428 of *IFIP Advances in Information and Communication Technology*, pages 446–459. Springer Berlin Heidelberg, 2014.

[3] Ann Cavoukian. Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices. Technical report, 2009.

[4] Ann Cavoukian and Jeff Jonas. Privacy by Design in the Age of Big Data. Technical report, Information and Privacy Commissioner, Ontario, Canada, 2012.

[5] ISO/IEC 29100. Information technology – Security techniques – Privacy framework. Technical report, 2011.

[6] David Wright and Charles Raab. Privacy principles, risks and harms. *International Review of Law, Computers and Technology*, 28(3):277–298, 2014.

[7] Fred H Cate. The Failure of Fair Information Practice Principles. In *Consumer Protection in the Age of the 'Information Economy'*, pages 341–377. 2006.

[8] Danie E. Oleary. Some Privacy Issues in Knowledge Discovery: The OECD Personal Privacy Guidelines. *IEEE Expert-Intelligent Systems and their Applications*, 10(2):48–59, 1995.

[9] Martin Rost and Kirsten Bock. Privacy by Design and the New Protection Goals. *DuD, January*, (November 2009):1–9, 2011.

[10] Gina Fisk, Calvin Ardi, Neale Pickett, John Heidemann, Mike Fisk, and Christos Papadopoulos. Privacy principles for sharing cyber security data. In *Proceedings - 2015 IEEE Security and Privacy Workshops, SPW 2015*, pages 193–197, 2015.