LEGAL DESIGN PATTERNS FOR PRIVACY

Helena Haapio / Margaret Hagan / Monica Palmirani / Arianna Rossi

Associate Professor of Business Law, University of Vaasa / International Contract Counsel, Lexpert Ltd
Pohjoisranta 20, 00170 Helsinki, FI
helena.haapio@lexpert.com; http://www.uva.fi/en/profile/?view=1041511 / http://www.lexpert.com

Director, Legal Design Lab, Stanford Center on the Legal Profession / Lecturer, Stanford Institute of Design, Stanford Law School
559 Nathan Abbott Way, 94035 Stanford, USA
mdhagan@stanford.edu; http://www.margarethagan.com

Associate Professor, Department of Legal Studies, University of Bologna / Research Fellow, CIRSFID, University of Bologna
Via Galliera 3, 40121 Bologna, IT
monica.palmirani@unibo.it

LAST-JD PhD Candidate, CIRSFID, University of Bologna
Via Galliera 3, 40121 Bologna, IT
arianna.rossi15@unibo.it

Abstract:	*Fulfilling the legal requirements of mandated disclosure is a challenge in many contexts. Privacy communication is no exception, especially for those who seek to effectively inform individuals about the use of their data. Lawyers across countries and industries are facing recurring problems when (re)writing privacy notices and terms. Visual and interactive design patterns have been suggested as the solution, yet our analysis shows that they are lacking on most privacy policies. This indicates the need for standardization and an actionable pattern library, which we propose in this paper.*

1. Introduction

One top priority of the General Data Protection Regulation (GDPR) is empowering individuals (or data subjects) to be informed about and in control of the use of their personal data. In fact, the data-driven economy fosters unbalanced relations between the entities that gather and process personal information and the individuals who are often unaware of the extent and the significance of the processing.[1] However, the principle of transparency[2] mandates data controllers to disclose complete and accurate information[3] about the modalities and purposes of their practices, and about data subjects' rights. This information (usually contained in a privacy policy) is deemed necessary to allow data subjects to understand, give consent to, and, if necessary, challenge the operations carried out on their data.[4] Transparency is also a critical element to increase individuals' trust in the data controller and therefore willingness to provide personal information.[5]

However, privacy communication tends to be «too long, overly legalistic, uninformative and unhelpful».[6] The complexity and the amount of information provided are so excessive that most of the time individuals do not

---

[1] DANEZIS ET AL. 2014.

[2] Under the GDPR, transparency becomes a fundamental aspect of the principles of lawfulness and fairness of the processing of personal data. *See* GDPR, Article 12, and ARTICLE 29 DATA PROTECTION WORKING PARTY 2017. *See also* EUROPEAN COMMISSION 2017, Article 8.

[3] The same applies to any communication addressed to data subjects, such as the communication of a personal data breach, *see* GDPR, Article 34.

[4] ARTICLE 29 DATA PROTECTION WORKING PARTY 2017.

[5] *See, e.g.* TADDEI/CONTENA 2013, WU ET AL. 2012.

[6] PEDDER 2016. *See also* ICO 2016.

read or understand the notices.[7] To fulfill the legal requirement of mandated disclosure, instead of effectively informing individuals about the use of their data, such notices are usually written «*by* lawyers *for* lawyers». Traditionally, they tend to focus on content and precision, much less on the needs of the users: the people who are impacted by or need to work with the text – mostly non-lawyers.[8]

Nevertheless, a major shift seems to be occurring: «[t]he concept of transparency in the GDPR is user-centric rather than legalistic»[9]. It is not only mandatory to disclose certain information about data practices,[10] but even the comprehensibility and presentation of that information assume a central role to demonstrate compliance and its quality should even be empirically evaluated.[11] These requirements pose an additional burden on data controllers, who will also need to comply with several other newly introduced obligations by May 2018.

In recent years, researchers and practitioners have started to explore innovative ways of communicating and presenting privacy information: layered notices, color coding, privacy icons, nutrition labels, dashboards, videos, even animations.[12] Although a number of experiments exist, they are scattered and not necessarily easy to find and replicate. Moreover, a tension exists between legal-friendly, business-friendly, and user-friendly approaches. How can solution developers serve the needs of business, secure transparency and data protection for individuals, while providing compliant and legally sound solutions?

We advocate the use of *design patterns*,[13] re-usable forms of a solution to a frequent problem – something that practitioners in many fields develop, collect, and then share in pattern libraries.[14] Design patterns offer many advantages: for people working on the same problem to communicate with each other; for people working on similar challenges in different domains to share knowledge and innovations; and for setting standards and best practices on how best to address a problem.[15] In our previous work, we have looked into *legal design patterns*[16] and *design patterns for contracts*[17]. This paper explores the application of design patterns to privacy and proposes a *design pattern library* where mechanisms focusing on privacy communication can be collected, integrated, and discussed.

2. Previous Privacy Design Pattern Work

Our work is not the first time that design patterns have been proposed for privacy communication. There are initial efforts to standardize the presentation of how terms and choices are communicated, as well as some pattern libraries for various visual design and engineering choices that may improve users' understanding of

---

[7] *See, e.g.* Calo 2012, European Commission et al. 2015, Reidenberg et al. 2015, Solove 2013. For a discussion on mandated disclosure, not only confined to privacy, *see* Ben-Shahar/Schneider 2014.

[8] End user license agreements, terms of service, and contract terms present similar shortcomings. *See, e.g.,* Mahler 2013, Haapio 2013, Conboy 2014, Mitchell 2015 and 2017, Haapio/Barton 2017.

[9] Article 29 Data Protection Working Party 2017, p. 6.

[10] *See* GDPR, Articles 13 and 14.

[11] Article 29 Data Protection Working Party 2017.

[12] *See, e.g.*, Hoepman 2014, Hagan 2016, Rossi/Palmirani 2017, Edwards/Abel 2014, Raskin 2009 and Lannerö 2013. *See also* good (and bad) examples of privacy notices available at the Information Commissioner's Office (ICO) website at https://ico.org.uk/ (all Websites last accessed on 2 January 2018) under the sections Privacy Notices in Practice and Where should you deliver privacy information to individuals? ICO is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. – ICO 2016, the ICO code of practice, provides guidance to organizations on how to make privacy notices more engaging and effective for individuals while emphasizing the importance of greater choice and control over what is done with their data.

[13] *See, e.g.,* Alexander et al. 1977, Alexander 1979, Gamma et al. 1994, Tidwell 2014, Waller/Delin 2011, and Pan/Stolterman 2013. For a timeline capturing many of the key points in the history of design patterns (albeit not in information design or contract design), *see* Malone 2017.

[14] For what concerns privacy and security design patterns, *see, e.g.* https://privacypatterns.eu, https://privacypatterns.org, Diamantopoulou et al. 2017, Doty/Gupta 2013, Graf et al.2010, Hoepman 2014, Romanosky et al. 2006.

[15] Haapio/Hagan 2016.

[16] Hagan 2017.

[17] Haapio/Hagan 2016, Haapio/Passera (forthcoming), Waller et al. 2016.

the privacy terms. In some instances there are single mechanisms of communication that are proposed as a new solution template, like visual icon sets;[18] layered notices that come in stages, like summary tables or nutrition labels;[19] videos explaining the terms;[20] vetted text templates;[21] and gamification.[22]

Other initiatives have begun to more explicitly craft a pattern language that collects many separate privacy communication solutions into a set, covering visual, interaction, evaluation, and code-based strategies.[23] Some privacy scholars have delineated the design space for privacy communication, that make explicit the different mechanisms that might be used to improve notice – suggesting many new patterns that could be used.[24] There are more technical design patterns that concern the construction of the system, rather than the communication to the user.[25] Others have warned of possible consumer harm from this work, via anti-patterns, when standard patterns are misapplied to content, thus undermining the communication.[26]

3. Our Exploratory Design Work to Identify Patterns

We drafted a first version of privacy design patterns based on our own exploratory workshops for communicating privacy concepts, and then a review of top websites to derive patterns based on current practices in use. We held a series of privacy policy design workshops – in May 2014 around financial websites' terms of service;[27] in Autumn 2015 on mobile phones' communication of apps' privacy;[28] and in July 2017 on GDPR communication.[29] In those workshops, teams of students and lawyers generated new ways to communicate privacy terms of service. We then analyzed their prototypes to identify the most common patterns that emerged as promising innovations. The following design patterns emerged: **visual iconography** that can flag if a certain issue or practice is present; **staging** a walk-through the terms, step-by-step; allowing users to choose a representative **persona,** which then would customize which terms they should pay most attention to; **gamification** of the terms, being quizzed about what the terms are; a **dashboard control center** of the terms, through which a user can continuously check in on what terms apply and what actions they can take; and **character-based explanations** of the terms, through stories. Each of them went through qualitative focus group testing inside the workshop, and received high marks for usability and engagement. We collected these as near-term possible patterns, even if they are not in current use.

To better understand the currently deployed privacy design patterns in use, in late 2017, our team of researchers evaluated what design patterns were in use on leading websites. We chose a sample of 152 websites based on the Alexa rankings of the most trafficked sites.[30] We selected a mixture of different industries, including music, technology, consumer goods, sports, social media, real estate, travel, and restaurants, and excluding pornography sites. For each of these websites, a team of researchers manually reviewed its privacy policy web

---

[18] *See e.g.* Raskin 2009, Holtz/Nocun/Hansen 2010, Moskowitz & Raskin 2011, HIIT 2016.

[19] *See* Kelley et al. 2009.

[20] *See* videos at LinkedIn (https://www.linkedin.com/legal/privacy-policy), the Guardian (https://www.theguardian.com/help/privacy-policy), and O2 (https://www.o2.co.uk/termsandconditions/privacy-policy). *See also* video on the GoAnimate website at ico.org.uk/PNvideo.

[21] *See* the International Regulatory Strategy Group's templated GDPR text, https://www.irsg.co.uk/resources-and-commentary/irsg-example-gdpr-ready-processor-terms/.

[22] *See* company Zynga's PrivacyVille game https://www.zynga.com/privacy/privacyville.

[23] PrivacyPatterns.org and PrivacyPatterns.eu have assembled a mixture of engineering and design mechanisms to present privacy terms. The CommonTerms project proposes five big pattern categories to improve privacy communications, http://www.commonterms.net/conclusions/.

[24] Schaub et al. 2015.

[25] Romanosky et al. 2006.

[26] Doty/Gupta 2013

[27] Hagan et al. 2014.

[28] Driscoll 2016.

[29] Legal Design Lab 2017.

[30] *See* the rankings https://www.alexa.com/siteinfo.

page on a desktop computer, along with any related privacy-related pages on the site. The researchers were focused on what visual, interaction, or communication mechanisms were in use on the page to communicate the policy in more user-friendly ways.

Our analysis showed a lack of visual or interactive mechanisms in use on most privacy policies.[31] Only 9% of the sites had any visuals. Over 76% had no color. Only 37% of sites had page jumps, to allow for quick access to certain terms or topics; and only 37% had a summary table or paragraph, akin to a layered disclosure. The only prominent mechanism in use was headings and division markers, with 86% of sites using them to demarcate terms. Our design review demonstrates that most proposed visual or interactive design patterns have not been embraced by practitioners. This could indicate the need for more standardization and an actionable pattern library, rather than the current fragmented collection of proposed mechanisms and libraries. It certainly indicates the need for more research of privacy communicators, to understand why they currently do not use the design patterns and what pattern library might work for them.

4. Our Proposal for a Privacy Communication Design Pattern Library

The GDPR puts effective privacy information at the center of data controllers' obligations, but our analysis shows that even the major players still rely on poor and inadequate communicative strategies. We propose a Privacy Design Pattern Library[32] where mechanisms focusing on privacy communication that are being developed and experimented throughout the world can be collected, integrated, and discussed. The core of the library contains not only existing patterns, but also proposed patterns that we or other researchers have developed, together with information about context of use and concrete examples. We hope to engage the vibrant privacy community in this collective effort to produce and share reusable solutions that will make data subjects more aware about the use of their data and their rights, and at the same time will help data controllers to be as transparent as the GDPR mandates. The flaws of traditional privacy communication are well known and well documented. Solutions have been developed and experimented, but have not met widespread adoption: let's change this. This paper is a first step towards this goal.

It is also necessary to keep an eye towards the future. Our way of interacting with legal information is radically changing: screens are becoming smaller and smaller or are even disappearing, while Augmented and Virtual Reality will enter our lives soon. New media will need innovative and appropriate design patterns that will be able to communicate privacy efficiently and successfully in a world not made of documents anymore.

5. References

ALEXANDER, CHRISTOPHER, The Timeless Way of Building, Vol. 1. Oxford University Press, New York 1979.

ALEXANDER, CHRISTOPHER/ISHIKAWA, SARA/SILVERSTEIN, MURRAY/JACOBSON, MAX/FIKSDAHL-KING, INGRID/ANGEL, SHLOMO, A Pattern Language – Towns, Buildings, Construction, Oxford University Press, New York 1977.

ARTICLE 29 DATA PROTECTION WORKING PARTY, Guidelines on Transparency under Regulation 2016/679, 17/EN WP 260, 2017. http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850.

BEN-SHAHAR, OMRI/SCHNEIDER, CARL E., More Than You Wanted to Know: the Failure of Mandated Disclosure. Princeton University Press, 2014.

CALO, M. RYAN, Against Notice Skepticism in Privacy (and Elsewhere). Notre Dame Law Review, Vol. 87, No. 3, 2012, p. 1027–1072.

CONBOY, KEVIN, Diagramming Transactions: Some Modest Proposals and a Few Suggested Rules, Transactions: Tennessee Journal of Business Law, Vol. 16, 2014, p. 91–108.

---

[31]   Contact Legal Design Lab for access to our analysis records and full list of sites, at mdhagan@stanford.edu.

[32]   http://www.legaltechdesign.com/communication-design/legal-design-pattern-libraries/privacy-design-pattern-library/; *see also* http://www.legaltechdesign.com/communication-design/legal-design-pattern-libraries/.

Danezis, George/Domingo-Ferrer, Josep/Hansen, Marit/Hoepman, Jaap-Henk/le Métayer, Daniel/Tirtea, Rodica/Schiffner, Stefan, Privacy and Data Protection by Design – from Policy to Engineering. December 2014. https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design/at_download/fullReport.

Diamantopoulou, Vasiliki/Kalloniatis, Christos/Gritzalis, Stefanos/Mouratidis, Haralambos, Supporting Privacy by Design Using Privacy Process Patterns, IFIP International Conference on ICT Systems Security and Privacy Protection, Springer, 2017, p. 491–505.

Doty, Nick/Gupta, Mohit, Privacy Design Patterns and Anti-Patterns, Trustbusters Workshop at the Symposium on Usable Privacy and Security, 2013.

Driscoll, Sharon, Applying Design Thinking to Law, Stanford Lawyer, Issue 94, July 2016, https://law.stanford.edu/stanford-lawyer/articles/legal-design-lab-consumer-contracts/.

Edwards, Lilian/Abel, Wiebke, The Use of Privacy Icons and Standard Contract Terms for Generating Consumer Trust and Confidence in Digital Services. CREATe Working Paper 2014/15. https://zenodo.org/record/12506/files/CREATe-Working-Paper-2014-15.pdf, 2014.

European Commission, Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). COM(2017) 10 final, 2017/0003 (COD), Brussels 10 January 2017. http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241.

European Commission/Directorate-General for Justice and Consumers/Directorate-General for Communication, Special Eurobarometer 431: Data Protection, TNS Opinion and Social, S2075_83_1_431_ENG, 2015. https://data.europa.eu/euodp/en/data/dataset/S2075_83_1_431_ENG.

Gamma, Erich/Helm, Richard/Johnson, Ralph/Vlissides, John, Design Patterns: Elements of Reusable Object-Oriented Software. Addison-Wesley Professional, 1994.

Graf, Cornelia/Wolkerstorfer, Peter/Geven, Arjan/Tscheligi, Manfred, A Pattern Collection for Privacy Enhancing Technology. In: Proceedings of PATTERNS 2010: The Second International Conferences on Pervasive Patterns and Applications, 21–26 November 2010, Lisbon, Portugal, p. 72–77, https://www.thinkmind.org/download_full.php?instance=PATTERNS+2010.

Haapio, Helena, Next Generation Contracts: A Paradigm Shift. Lexpert Ltd, Helsinki 2013.

Haapio, Helena/Barton, Thomas D., Business-Friendly Contracting: How Simplification and Visualization Can Help Bring It to Practice. In: Jacob, Kaj, Schindler Dierk & Strathausen Roger (Eds), Liquid Legal. Management for Professionals. Springer, Cham 2017, p. 371–396.

Haapio, Helena/Hagan, Margaret, Design Patterns for Contracts. In Schweighofer, Erich, Kummer, Franz, Hötzendorfer, Walter & Borges, Georg (Eds), Networks. Proceedings of the 19th International Legal Informatics Symposium IRIS 2016. Österreichische Computer Gesellschaft OCG / books@ocg.at, Wien 2016, p. 381–388.

Haapio, Helena/Passera, Stefania, Contracts as Interfaces: Exploring Visual Representation Patterns In Contract Design. In: Katz, Daniel Martin, Bommarito, Michael & Dolin, Ron (Eds), Legal Informatics. Cambridge University Press, forthcoming.

Hagan, Margaret D., User-Centered Privacy Communication Design. In: Proceedings of the Symposium on Usable Privacy and Security (SOUPS) 2016, Denver, Colorado, 22–24 June 2016. https://ssrn.com/abstract=2981075.

Hagan, Margaret, Law by Design, 2017. http://www.lawbydesign.co.

Hagan, Margaret D./Gavis, Alex/Ozenc, Kursat, Designing Legal Communications that Resonate, VoxPopuLII Blog, Cornell University Law School Legal Information Institute, 5 September 2014.

Helsinki Institute for Information Technology HIIT, Consent Experience Graphics, 30 August 2016, https://github.com/HIIT/mydata-sdk/tree/master/graphics.

Hoepman, Jaap-Henk, Privacy Design Strategies. In: Cuppens-Boulahia, Nora, Cuppens, Frédéric, Jajodia, Sushil, Abou El Kalam, Anas & Sans, Thierry (Eds), ICT Systems Security and Privacy Protection. Proceedings of the 29th IFIP TC 11 International Conference, SEC 2014, Marrakech, Morocco, 2–4 June 2014. IFIP Advances in Information and Communication Technology, Vol. 428. Springer, Berlin, Heidelberg 2014, p. 446–459.

Holtz, Leif-Erik/Nocun, Katharina/Hansen, Marit, Towards Displaying Privacy Information with Icons. In: Camenisch, Ian, Crispo, Bruno, Fischner-Hubner, Simone, Leenes, Ronald & Russello, Giovanni (Eds.), IFIP PrimeLife International Summer School on Privacy and Identity Management for Life. Springer, Berlin, Heidelberg 2010, p. 338–348.

INFORMATION COMMISSIONER'S OFFICE (ICO), Privacy notices, transparency and control. A code of practice on communicating privacy information to individuals. ICO, 7 October 2016, 1.0.34. PDF report downloaded from https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/.

KELLEY, PATRICK G./BRESEE, JOANNA/CRANOR, LORRIE F./REEDER, ROBERT W., A «Nutrition Label» for Privacy. In: Proceedings of the 5th Symposium on Usable Privacy and Security SOUPS 2009, Mountain View, CA.

LANNERÖ, PÄR, Fighting the Biggest Lies on the Internet. Common terms beta proposal 30 April 2013. Metamatrix, Stockholm. http://www.commonterms.net/commonterms_beta_proposal.pdf.

LEGAL DESIGN LAB, Design Workshop for EU General Data Protection Regulation, July 2017, http://www.legaltech design.com/design-workshop-for-eu-general-data-protection-regulation/.

MAHLER, TOBIAS, A graphical user-interface for legal texts? In: Svantesson, Dan Jerker B. & Greenstein, Stanley (Eds.), Internationalisation of Law in the Digital Information Society. Nordic Yearbook of Law and Informatics 2010–2012. Ex Tuto Publishing, Copenhagen 2013, p. 311–327.

MALONE, ERIN, A History of Patterns in User Experience Design. Filling in some missing pieces. Tangible UX, 31 March 2017, https://medium.com/tangible-ux/a-history-of-patterns-in-user-experience-design-f21f7eaabb83.

MITCHELL, JAY A., Whiteboard and Black-Letter: Visual Communication in Commercial Contracts. Stanford Public Law Working Paper, 22 October 2017. (forthcoming in University of Pennsylvania Journal of Business Law, Vol. 20), https://ssrn.com/abstract=3057075.

MITCHELL, JAY A., Putting some product into work-product: corporate lawyers learning from designers. Berkeley Business Law Journal, Vol. 12, Issue 1, 2015, p. 1–44. http://scholarship.law.berkeley.edu/bblj/vol12/iss1/1/.

MOSKOWITZ, BEN/RASKIN, AZA, Privacy Icons. Mozilla Wiki, 2011, https://wiki.mozilla.org/Privacy_Icons.

PAN, YUE/STOLTERMAN, ERIK, Pattern Language and HCI: Expectations and Experiences. In: CHI 2013 Extended Abstracts on Human Factors in Computing Systems. Association of Computing Machinery (ACM), New York (NY) 2013, pp. 1989–1998.

PEDDER, JO, Revised code looks at privacy notices. Information Commissioner's Office Blog, 2 February 2016. https://iconewsblog.org.uk/2016/02/02/revised-code-looks-at-privacy-notices/.

RASKIN, AZA, Making Privacy Policies Not Suck. Blog post, 30 October 2009. http://www.azarask.in/blog/post/making-privacy-policies-not-suck/.

REIDENBERG, JOEL R./BREAUX, TRAVIS/CRANOR, LORRIE F./FRENCH, BRIAN M., Disagreeable Privacy Policies: Mismatches between Meaning and Users' Understanding. Berkeley Technology Law Journal, Vol. 30, No. 1, 2015, p. 39–88.

ROMANOSKY, SASHA/ACQUISTI, ALESSANDRO/HONG, JASON/CRANOR, LORRIE FAITH/FRIEDMAN, BATYA, Privacy Patterns for Online Interactions. Proceedings of the 2006 conference on Pattern languages on programs. ACM, 2006, p. 1–15.

ROSSI, ARIANNA/PALMIRANI, MONICA, A Visualization Approach for Adaptive Consent in the European Data Protection Framework. In: Parycek, Peter & Edelmann, Noella (Eds), Proceedings of the 7th International Conference for E-Democracy and Open Government (CeDEM), Krems, Austria 2017, p. 159–170.

SCHAUB, FLORIAN/BALEBAKO, REBECCA/ DURITY, ADAM/ CRANOR, LORRIE, A Design Space for Effective Privacy Notices. In: Proceedings of Symposium on Usable Privacy and Security SOUPS 2015, Ottawa.

SOLOVE, DANIEL J., Privacy Self-Management and the Consent Dilemma. Harvard Law Review, Vol. 126, 2013, p. 1880–1903.

TADDEI, STEFANO/CONTENA, BASTIANINA, Privacy, Trust, and Control: Which Relationships with Online Self-Disclosure?, Computers in Human Behavior, 2013, Vol. 29, No. 3, p. 821–826.

TIDWELL, JENIFER, Designing Interfaces. 2nd edition, O'Reilly Media, Sebastopol (CA) 2014.

WALLER, ROBERT/DELIN, JUDY, Towards a pattern language approach to document description. Simplification Center Technical paper 4, April 2011. https://www.reading.ac.uk/web/FILES/simplification/tech_paper_4.pdf.

WALLER, ROB/WALLER, JENNY/HAAPIO, HELENA/CRAG, GARY/MORRISSEAU, SANDI, Cooperation through Clarity: Designing Simplified Contracts. Journal of Strategic Contracting and Negotiation, Vol. 2, No. 1–2, March/June 2016, p. 48–68.

WU, KUANG-WEN/HUANG, SHIAO YAN/YEN, DAVID C./POPOVA, IRINA, The Effect of Online Privacy Policy on Consumer Privacy Concern and Trust. Computers in Human Behaviour, Vol. 28, No. 3, 2012, p. 889–897.