TRUSTWORTHY PRIVACY INDICATORS: GRADES, LABELS, CERTIFICATIONS, AND DASHBOARDS[*]

JOEL R. REIDENBERG
Stanley D. and Nikki Waxberg Chair and Professor of Law,
Fordham Law School
Academic Director, Fordham CLIP

N. CAMERON RUSSELL
Executive Director, Fordham CLIP

VLAD HERTA
Project Fellow, Fordham CLIP

WILLIAM SIERRA-ROCAFORT
Project Fellow, Fordham CLIP

THOMAS B. NORTON
Privacy Fellow, Fordham CLIP

ABSTRACT

Despite numerous groups' efforts to score, grade, label, and rate the privacy of websites, apps, and network-connected devices, these attempts at privacy indicators have, thus far, not been widely adopted. Privacy policies, however, remain long, complex, and impractical for consumers. Communicating in some short-hand form, synthesized privacy content is now crucial to empower internet users and provide them more meaningful notice, as well as nudge consumers and data processors toward more meaningful privacy. Indeed, on the basis of these needs, the National Institute of Standards and Technology and the Federal Trade Commission in the United States, as well as lawmakers and policymakers in the

[*] © 2019 Fordham Center on Law and Information Policy (Fordham CLIP). The authors would like to thank Fordham CLIP Project Fellows Antoine Bon, Sam Borenzweig, Tim Carter, Elle Davis, and Stephanie Tallering for their assistance preparing this paper's Appendix materials and for providing research assistance on this project. The authors would also like to thank the participants at the USENIX SOUPS 2016 Workshop on Privacy Indicators for comments on our preliminary research and the participants at the 2018 Northeast Privacy Scholars Workshop, and Emily McReynolds in particular, for their thoughtful feedback on an earlier draft of this article. National Science Foundation Grant CNS-1330214 and a Fordham Faculty Fellowship supported work on this article.

European Union, have advocated for the development of privacy indicator systems.

Efforts to develop privacy grades, scores, labels, icons, certifications, seals, and dashboards have wrestled with various deficiencies and obstacles for the wide-scale deployment as meaningful and trustworthy privacy indicators. This paper seeks to identify and explain these deficiencies and obstacles that have hampered past and current attempts. With these lessons, the article then offers criteria that will need to be established in law and policy for trustworthy indicators to be successfully deployed and adopted through technological tools. The lack of standardization prevents user-recognizability and dependability in the online marketplace, diminishes the ability to create automated tools for privacy, and reduces incentives for consumers and industry to invest in privacy indicators. Flawed methods in selection and weighting of privacy evaluation criteria and issues interpreting language that is often ambiguous and vague jeopardize success and reliability when baked into an indicator of privacy protectiveness or invasiveness. Likewise, indicators fall short when those organizations rating or certifying the privacy practices are not objective, trustworthy, and sustainable.

Nonetheless, trustworthy privacy rating systems that are meaningful, accurate, and adoptable can be developed to assure effective and enduring empowerment of consumers. This paper proposes a framework using examples from prior and current attempts to create privacy indicator systems in order to provide a valuable resource for present-day, real world policymaking.

First, privacy rating systems need an objective and quantifiable basis that is fair and accountable to the public. Unlike previous efforts through industry self-regulation, if lawmakers and regulators establish standardized evaluation criteria for privacy practices and provide standards for how these criteria should be weighted in scoring techniques, the rating system will have public accountability with an objective, quantifiable basis. If automated rating mechanisms convey to users accepted descriptions of data practices or generate scores from privacy statements based on recognized criteria and weightings rather than from deductive conclusions, then this reduces interpretive issues with any privacy technology tool. Second, rating indicators should align with legal principles of contract interpretation and the existing legal defaults for the interpretation of silence in privacy policy language. Third, a standardized system of icons, along with guidelines as to where these should be located, will reduce the education and learning curve now necessary to understand and benefit from many different, inconsistent privacy indicator labeling systems. And lastly, privacy rating *evaluators must be impartial, honest, autonomous, and financially and operationally durable in order to be successful.*

TABLE OF CONTENTS

INTRODUCTION

Privacy policies are notoriously long, complex, and impractical for consumers. [1] To assist users of websites, internet platforms, mobile applications, and network-connected devices in evaluating privacy notices and gleaning useful information from them, many have tried to synthesize privacy content into short-hand indicators and some have tried to develop automated technological tools to create or display the indicators. These indicators include grades, scores, nutrition labels, ratings, certifications, and dashboards.[2] Despite numerous groups' efforts to score, grade, label, and rate the privacy of websites, apps, and network-connected devices, these attempts at privacy indicators have, thus far, not been widely adopted.[3]

Privacy policies, however, remain long, complex, and impractical for consumers. The ever-growing Internet of Things and growth of Big Data continue to undermine our reliance on long written disclosures, because data practices increase in complexity raising many difficulties for an accurate description that is meaningful to consumers. Communicating in some short-hand form, synthesized privacy content is now crucial to empower internet users and provide them more meaningful notice, as well as nudge consumers and data processors toward more meaningful privacy. This highlights the need to satisfy privacy concerns *ex ante* to assure trust in online systems.

In the modern network-connected world, privacy notices are failing to provide meaningful transparency for users, and many are hastening to move toward short-hand indicators of synthesized privacy policy content. The National Institute of Standards and Technology (NIST) and the Federal Trade Commission (FTC), for example, have explored solutions to improve notice and choice and synthesize statements of privacy practices.[4] This

[1] *See, e.g.*, Patrick Gage Kelley et al., *A "Nutrition Label" for Privacy*, 2009 PROC. 5TH SYMP. ON USABLE PRIVACY & SECURITY (SOUPS) no. 4, https://cups.cs.cmu.edu/soups/2009/proceedings/a4-kelley.pdf [https://perma.cc/A59B-G7ME].

[2] When we use "indicators" in this paper, we mean the broader category of aspects of privacy policies that are synthesized, extracted, or interpreted, and which are visually communicated to users. Privacy grades, scores, nutrition labels, ratings, certifications, and aspects of privacy dashboards are all privacy indicators, but this is by no means an exhaustive list. In addition, as demonstrated by many of the examples in this paper, privacy indicators can combine two or more different approaches to visually depict privacy. For example, one privacy indicator may include both privacy labeling and scoring.

[3] *See, e.g.*, Manoj Hastak & Mary J. Culnan, *Online Behavioral Advertising "Icon" Study*, FUTURE OF PRIVACY FORUM 2–3 (Jan. 25, 2010), https://fpf.org/wp-content/uploads/2016/06/Ad_Icon_Study.pdf [https://perma.cc/E8T4-BX5L] (concluding that icons representing behavioral advertising practices were confusing, and finding it unclear how well online behavioral advertising icons could actually communicate with users); *see also infra* Part 0.

[4] *See, e.g.*, *infra* notes 10–11 and accompanying text. The Federal Communications Commission has also attempted to regulate privacy notices in the telecommunications sector. *See* Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 81 Fed. Reg. 87,274, 87,275 (Dec. 2, 2016) (requiring "carriers to provide privacy notices that clearly and accurately inform customers about what confidential information the carriers collect, how they use it,

paper seeks to provide a valuable resource for not only the legal community, but also for businesses and policymakers who are focused on improving privacy online.

Over the years, efforts to develop privacy grades, scores, labels, icons, certifications, seals, and dashboards have wrestled with various deficiencies and obstacles for the wide-scale deployment as meaningful and trustworthy privacy indicators. This paper identifies and explains the deficiencies and obstacles that have hampered past and current attempts to develop and deploy trustworthy and meaningful privacy indicators. Taking these problems as lessons, the paper offers criteria that can be established in law and policy so that trustworthy and meaningful indicators can be successfully deployed and adopted through technological tools.

To provide context, Section I describes the goals for privacy indicators. These goals are distilled from various past and current attempts at the generation of online privacy indicators. Despite differing methodologies and approaches, online privacy indicators have set out to achieve three similar goals: to provide consumers with more meaningful notice; to empower consumers; and to nudge data processors to improve online privacy notices.

Section II contributes to the academic and industry dialogue a typology of online privacy indicators. Attempts to create meaningful and trustworthy privacy indicators from full-length privacy policies appear to fit into one or more of four categories: privacy grades or scores; privacy labels; privacy certifications or seals; and privacy dashboards. Section III then analyzes notable attempts at the creation and deployment of online privacy indicators to isolate the specific obstacles to the development of meaningful synthesized privacy policy content.

To overcome the obstacles identified in Section III, Section IV proposes a set of requirements for the successful deployment of privacy indicators. Indicators can adequately, accurately, and successfully synthesize online

under what circumstances they share it, and the categories of entities with which they will share it."). The broad ruling, which also covered topics like data security and customer consent, was nullified by Congress under the Congressional Review Act (CRA) in March of 2017. *See* S.J. Res. 34, 115th Cong., 131 Stat. 88 (2017); *see also* NIST'S INFO. SEC. & PRIVACY ADVISORY BD. (ISPAB), TOWARD A 21ST CENTURY FRAMEWORK FOR FEDERAL GOVERNMENT PRIVACY POLICY 36 (2009), https://csrc.nist.gov/Presentat ions/2009/ISPAB-Recommendations-to-OMB-Updating-Privacy-Law [https://perma.cc/T7WS-KU73] (recommending that Government privacy notices be standardized and use "layered notices" operating as snapshots making them "more readable to the general public"); NAT'L INST. OF STANDARDS & TECH., SPEC. PUB. NO. 800-53, SECURITY AND PRIVACY CONTROLS FOR INFORMATION SYSTEMS AND ORGANIZATION, rev. 5, at 37 (2017), https://csrc.nist.gov/csrc/media/publications/sp/800-53/rev-5/draft /documents/sp800-53r5-draft.pdf [https://perma.cc/4YAV-WTBQ] (calling for "[p]rivacy attributes, which . . . represent the basic properties or characteristics of an entity with respect to the management of personally identifiable information."). This project remains at its draft stage as of February 1, 2019. *Publication Schedule*, NIST, https://csrc.nist.gov/projects/risk-management/schedule [https://perma.cc/ 34CE-4FBH].

privacy content if: (1) lawmakers or regulators establish both standardized evaluation criteria for the privacy practices under consideration and appropriate weightings for scoring techniques; (2) in the analytical and interpretive approach, rating mechanisms must accurately convey to users the actual and demonstrable data practices, or else simply show without deductive reasoning what a privacy statement says according to recognized criteria including the legal principles of contract interpretation and legal defaults associated with the meaning of silence in privacy policy language; (3) lawmakers or regulators provide an imprimatur to a standardized system of icons along with guidelines as to where and how they should be displayed; and (4) privacy raters are impartial, honest, autonomous, and financially and operationally durable.

I. GOALS FOR PRIVACY INDICATORS

Many have tried to develop privacy indicators.[5] Such initiatives generally seek to achieve three common objectives: provide consumers with more meaningful notice, empower consumers, and nudge data processors to improve their privacy notices and practices. The three subsections below describe each of these goals.

A. More Meaningful Notice

One goal of privacy indicators is to offer more meaningful notice of privacy practices or privacy policy content. Research shows that while consumers express concern about their privacy online, few, if any, read online privacy policies.[6] This is because policies are often long, written in highly technical language, describe user website activities in ways that are incongruent with user understanding, and require a college education reading level.[7] Also, already elaborate data practices are gaining complexity.[8] Accordingly, the FTC, European Union (EU), academics, and industry stakeholders have advocated for and sought out ways to provide more meaningful notice about privacy policies to consumers through the use of labelling, rating, and grading schemes.[9]

[5] *See infra* Part 0.

[6] *See* Kelley et al., *supra* note 1, at 1.

[7] *See id.*

[8] *See, e.g.*, Jason Parms, *More Info, More Problems: Privacy and Security Issues in the Age of Big Data*, BUSINESS.COM (Feb. 22, 2017), https://www.business.com/articles/privacy-and-security-issues-in-the-age-of-big-data/ [https://perma.cc/XMK3-G4SH].

[9] *See, e.g.*, Lorrie Faith Cranor, *Necessary but Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice*, 10 J. ON TELECOMM. & HIGH TECH. L. 273, 277–95 (2012) (describing and analyzing government agency, academia and industry initiatives); Hugo Roy, *Why So Many Services*

In its 2017 *Privacy & Data Security Update*, the FTC stressed the importance of improved notice as a means for providing greater transparency.[10] In 2013, the FTC published a Mobile Privacy report recommending privacy dashboards and privacy icons as privacy enhancing tools to increase transparency.[11] This report suggests that a privacy dashboard tool "provides an easy way for [mobile app] consumers to determine which apps have access to which data and to revisit the choices they initially made about the apps."[12] Furthermore, according to the report, privacy icons "offer the ability to communicate key terms and concepts in a clear and easily digestible manner,"[13] thereby providing more meaningful notice. For example, Apple signals to consumers when an app is accessing their geolocation information by displaying an arrow-shaped icon in the top status bar.[14] Android uses a circular icon to convey the same information.[15]

The FTC's Mobile Privacy report also recommended that app trade associations explore developing standardized icons for more meaningful notice.[16] An example was an "icon [that would] appear[] in the top status bar of a smartphone, signal[ing] to a consumer that an app is collecting data by visually bursting three times and then glowing."[17] The icon would also allow users to pull down a menu providing more information about the collected data and privacy practices.[18] The FTC advised that developers disclose what types of information they collect and whether they share that information.[19] The report also encouraged developers to provide information on why the app is accessing a particular type of information.[20]

The European Union's General Data Protection Regulation (GDPR) came into effect on May 25, 2018. The GDPR requires transparency of processing and transparency of the purposes of data use through notice to

Have "No Class Yet", ToS;DR (Nov. 19, 2012), https://tosdr.org/blog/why-no-class-yet.html [https://perma.cc/7XPC-2GFQ]; Kelley et al., *supra* note 1.

[10] *See* FED. TRADE COMM'N, PRIVACY & DATA SECURITY UPDATE (2017), https://www.ftc.gov/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives [https://perma.cc/GZ6V-U9N7] (highlighting initiatives, rulings, and comments advocating or mandating the expansion of privacy policy and practices noticing requirements and increasing their transparency).

[11] *See* FED. TRADE COMM'N, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY 16–18 (2013), https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf [https://perma.cc/HK2N-48EG] [hereinafter FED. TRADE COMM'N, MOBILE PRIVACY REPORT].

[12] *Id.* at 16.

[13] *Id.* at 17.

[14] *Id.*

[15] *Id.* at 18.

[16] *Id.* at 25.

[17] *Id.*

[18] *Id.*

[19] *Id.* at 26.

[20] *Id.*

data subjects.[21] Transparency means that information about the processing of personal data be "concise, easily accessible and easy to understand . . . and, additionally, where appropriate, visualisation be used."[22] In cases where the lawfulness of processing relies on consent, entities seeking to collect and process personal data from inside or outside the EU must also provide "any information . . . relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language . . . . in writing, or by other means."[23] Consent must be informed,[24] compelling data controllers to make privacy policy disclosures. To achieve proper notice, the GDPR suggests the use of "standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing."[25] Many websites have already developed downloadable GDPR-tailored privacy icons.[26]

Academia, too, has produced privacy indicators designed to provide more meaningful notice. Professor Lorrie Cranor's "Nutrition Label" approach, for instance, seeks to provide "a clear, uniform, single-page summary of a company's privacy policy."[27] The summary seeks to enable users to efficiently glean information, allowing for easier comparison of privacy notices, and shorten the amount of time required to read and comprehend those notices.[28] Cranor's research found that the nutrition label approach possessed a number of notice-providing advantages over traditional text privacy policies.[29]

Lastly, industry stakeholders have developed grading schemes intended to provide more meaningful notice to consumers. For example, CommonTerms is an initiative intended to make online legal policies more accessible to consumers.[30] ToS;DR (or Terms of Service; Didn't Read) created a process that rates and analyzes various websites' terms of service and privacy policies to inform users of their rights under those terms.[31]

[21] *See* Regulation 2016/679, art. 12–14, 2016 O.J. (L 119) 1, 39–42 [hereinafter GDPR].

[22] *Id.* pmbl. ¶ 58, at 11.

[23] *Id.* art. 12(1), at 39.

[24] *Id.* art. 4(11), at 34 ("'[C]onsent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.").

[25] *Id.* art. 12(7), at 40.

[26] *See, e.g.*, Ieva Andriuleviciute, *GDPR Icons*, ICONFINDER BLOG (Apr. 20, 2018), https://blog.iconfinder.com/gdpr-icons-d13900ce9296 [https://perma.cc/LWN3-YLQD].

[27] *See* Kelley et al., *supra* note 1, at 1.

[28] *See id.*

[29] *See* Cranor, *supra* note 9, at 288.

[30] *See Towards Better Online Terms & Conditions*, COMMONTERMS, http://commont erms.net/ [https://perma.cc/895R-2MAT].

[31] *See Classification*, TOS;DR, https://tosdr.org/classification.html [https://perma.cc/NRU7-7CCN].

Similarly, Mozilla's privacy icon initiative allowed users to learn whether and how a particular site used their data by affixing simple icons to the top of the site's privacy policy.[32] According to the project development team, the icons provide "companies [with] the flexibility needed to create comprehensive, detailed, and meaningful policies."[33] PrivacyGrade.org seeks to raise awareness on smartphone app functions that may affect users' privacy by providing detailed information about a particular app's privacy-related practices and assigning the practices a grade.[34]

B. Consumer Empowerment

Even if consumers do read and understand lengthy and verbose privacy agreements, they do not believe they have a choice when it comes to their privacy.[35] Thus, some attempts to create privacy indicators have focused on empowering consumers to make choices based on privacy preferences. The aforementioned FTC Mobile Privacy report urges developers to offer privacy dashboards, including an on/off button, as tools to empower consumers to make better choices.[36] The GDPR requires entities to integrate Privacy-by-Design (PbD) to give EU residents greater control over their personal information.[37] PbD is the practice of integrating privacy principles and controls into business systems and technologies as they are being developed.[38]

Industry stakeholders have offered consumers more opportunities for control and empowerment. For example, ToS;DR aims to give users improved control over their data and privacy.[39] Likewise, Disconnect.me's icons and privacy tools allow users to control access to their personal information.[40] Similarly, the Better Business Bureau (BBB) certifications are built around the BBB Standards of Trust, designed to "enhance customer trust and confidence in business."[41] Reeling from the Cambridge Analytica

[32] *See Privacy Icons*, MOZILLA WIKI, https://wiki.mozilla.org/Privacy_Icons [https://perma.cc/8PHZ-9WCB] (last updated June 28, 2011).

[33] *Id.*

[34] *See FAQ*, PRIVACYGRADE, http://privacygrade.org/faq [https://perma.cc/B9FG-3T2Y].

[35] *See* Kelley et al., *supra* note 1 at 1.

[36] *See* FED. TRADE COMM'N, MOBILE PRIVACY REPORT, *supra* note 11, at 26.

[37] *See* GDPR, *supra* note 21, art. 25, at 48.

[38] European Data Protection Supervisor, Opinion 5/2018, Preliminary Opinion on Privacy by Design (May 31, 2018), https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf [https://perma.cc/X2N4-HU4H].

[39] *About*, TOS;DR, https://tosdr.org/about.html [https://perma.cc/B6EB-6C4B].

[40] *See, e.g.*, Seth Fiegerman, *Disconnect.me Lets You Control Your Data Online*, MASHABLE (Apr. 17, 2013), http://mashable.com/2013/04/17/disconnect-me/#3e865wCgwgqt [https://perma.cc/FDB6-2XMC].

[41] *BBB Accreditation Standards*, BETTER BUS. BUREAU, https://www.bbb.org/bbb-accreditation-standards (last visited June 22, 2018).

data sharing scandal, Facebook has made multiple attempts to increase privacy policy transparency and enhance consumer control over privacy settings.[42]

C. Nudging Users and Data Processors Toward Privacy

Privacy indicators are also designed to nudge users and data processors to engage in more responsible privacy practices and decision-making.[43] "Nudging" is a behavioral science theory asserting that non-coercive, positive suggestions or reinforcements can affect decision-making more effectively than direct regulation or enforcement.[44] "Nudging" theory has already been applied in the realm of privacy.[45] For example, one study revealed that "merely priming Facebook users with questions about their online disclosure behavior and the visibility of their Facebook profiles was sufficient to trigger changes in their disclosure behavior."[46] Another study showed that online shoppers are more likely to purchase from websites that purport to engage in more privacy-protective practices and are even willing to pay a premium to do so.[47] Privacy indicators, then, can be an effective tool for influencing users' privacy choices.

Similarly, privacy seal or certification programs can influence businesses' or data processors' privacy practices. Certifying organizations such as TrustArc, BBBOnLine Privacy, or the Entertainment Software Ratings Board seals seek to require their licensees to implement certain fair information practices and to submit to various types of compliance monitoring before their seal can be displayed.[48] A seal or similar certification can be an effective marketing tool,[49] creating a strong incentive

[42] *See, e.g.*, Aric Jenkins, *Facebook Just Revealed 3 Major Changes to Its Privacy Settings*, TIME (Mar. 28, 2018), http://time.com/5218395/facebook-privacy-settings-changes-cambridge-analytica/ [https://perma.cc/9BUJ-SYLL].

[43] *See generally* Rebecca Balebako et al., *Nudging Users Towards Privacy on Mobile Devices*, 2011 PROC. 2D INT'L WORKSHOP ON PERSUASION, NUDGE, INFLUENCE & COERCION, ceur-ws.org/Vol-722/paper6.pdf [https://perma.cc/R6YW-Z86Y].

[44] *See generally* RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS (2008). One of the most frequently cited examples of the theory at work appears in Amsterdam's Schiphol Airport, where etchings of houseflies appear at the base of men's room urinals to "improve the aim." *Id.* at 3–4.

[45] *See generally* Balebako et al., *supra* note 43.

[46] *Id.* at 2 (citing Ralph Gross & Alessandro Acquisti, *Information Revelation and Privacy in Online Social Networks*, 2005 PROC. ACM WORKSHOP ON PRIVACY ELECTRONIC SOC'Y 71).

[47] *See* Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*, 22 INFO. SYS. RES. 254, 254 (2011).

[48] *See, e.g.*, *TRUSTe Privacy Program Standards*, TRUSTARC, https://www.trustarc.com/privacy-certification-standards/ [https://perma.cc/F9VL-U7PA]; *Monitoring & Consulting*, ENTM'T SOFTWARE RATING BD., http://www.esrb.org/privacy/monitoring_consulting.aspx [https://perma.cc/J6FV-PCLQ].

[49] *See, e.g.*, Tsai et al., *supra* note 47, at 256.

for data processors to earn certification and thereby purportedly comply with certifying organizations' privacy requirements.

II. TYPES OF ONLINE PRIVACY INDICATORS

Many have attempted to develop privacy indicators.[50] The majority can be classified into one or more of four categories: privacy grades or scores, privacy labels or icons, privacy certifications or seals, and privacy dashboards. *Privacy grades and scores* assess privacy policies and practices by giving them a summary indicator, such as a letter grade, numeric rating, or gold star. *Privacy labels* identify the existence, or absence, of certain privacy practices or consumer protections. *Privacy certifications and seals* vouch for a website or online service's compliance with certain legal or industry standards. *Privacy dashboards* seek to aggregate privacy assessments and actionable aspects in a single user-friendly place. This section examines each category in detail.

A. Privacy Grades and Scores

Some privacy indicators synthesize online privacy policy content into grades, scores, or other similar rating systems. Two notable examples are ToS;DR (Terms of Service; Didn't Read) and PrivacyGrade.org

ToS;DR analyzes and rates terms of service and privacy policies.[51] The ratings produced by ToS;DR are accessible on its website, as well as via a browser plugin which displays the class (*i.e.*, grade) when a user visits a website with a rating.[52] Inspired by the European Union's energy labels,[53] ToS;DR divides terms of service and privacy policy elements into twenty-four topics including Business Transfers, Notice of Changing Terms, Governance, Third Parties, and User Choice.[54] Topics are discussed on the ToS;DR public Google group and assigned a score based on participants' assessments.[55] The grade comes in the form of four "badges"—"Good,"

[50] The attempts at privacy indicators discussed in this paper and its Appendix are by no means exhaustive. For a more comprehensive catalog of attempts, see PÄR LANNERÖ, FIGHTING THE BIGGEST LIE ON THE INTERNET: COMMONTERMS BETA PROPOSAL (2013), http://www.commonterms.org/commonterms_beta_proposal.pdf [https://perma.cc/8HLS-NFU3]; Solon Barocas, *Parsing Privacy Policies*, http://solon.barocas.org/?page_id=200 [https://perma.cc/G 5XV-96KD].

[51] *See About*, TOS;DR, *supra* note 39.

[52] *See id.*

[53] Commission Delegated Regulation 1060/2010 of Sept. 28, 2010, Supplementing Directive 2010/30/EU of the European Parliament and of the Council with Regard to Energy Labeling of Household Refrigerating Appliances, 2011 O.J. (L314) 17.

[54] *See Topics*, TOS;DR, https://tosdr.org/topics.html [https://perma.cc/Y68H-ZLBK].

[55] *See Terms of Service; Didn't Read*, GOOGLE GROUPS, https://groups.google.com/forum/#!forum/tosdr [https://perma.cc/ZEA7-RAVZ].

"Bad," "Blocker," or "Neutral."[56] Once a service accrues "enough badges to assess the fairness of [its] terms for users,"[57] a classification is assigned ranging from Class A to Class E by reviewing the average scores of segmented sections.[58] Many ToS;DR-reviewed services have the "No Class Yet" designation assigned where the ToS;DR team "think[s] [it] need[s] more reviews on that specific service before [it] can fully assess it."[59]

Another example of a privacy scoring scheme is PrivacyGrade.org, which provides information about smartphone applications' privacy policies and practices by issuing letter grades ranging from A+ to D.[60] These scores represent the disparity between users' expectations of what are appropriate data and privacy practices in comparison with an application's function and actual practices.[61] A+ symbolizes little or no discrepancy, while D represents a wide divergence between expectations and practices.[62]

These grades are assigned by applying a proprietary privacy model to consumer survey data.[63] To obtain the data necessary to draw comparisons, participants in 2012 and 2014 research studies were shown apps and asked whether they expected those apps to collect personal information in light of the apps' primary function.[64] The privacy model divides the surveyed applications into four quartiles according to their divergence score.[65] Applications in each quartile receive a grade from A to D, in order beginning with the smallest divergency quartile.[66] PrivacyGrade.org concedes, however, that it does not compare data privacy policies to actual practices or to privacy policies of similar applications.[67] Additionally, PrivacyGrade.org does not compare the policies of applications with similar functions to determine whether different programs adhere to best practices within each's respective industry sector.[68]

[56] *See Classification*, TOS;DR, *supra* note 31.

[57] *Id.*

[58] *See Ratings*, TOS;DR, https://tosdr.org/index.html#services [https://perma.cc/3BB4-R8ZR].

[59] *See Roy*, *supra* note 9.

[60] *See FAQ*, PRIVACYGRADE, *supra* note 34.

[61] *See* Jialiu Lin et al., *Expectation and Purpose: Understanding Users' Mental Models of Mobile App Privacy Through Crowdsourcing*, 2012 PROC. 14TH ACM INT'L CONF. ON UBIQUITOUS COMPUTING (UBICOMP) 501 [hereinafter Lin et al., 2012]; Jialiu Lin et al., *Modeling Users' Mobile App Privacy Preferences: Restoring Usability in a Sea of Permission Settings*, 2014 PROC. 10TH SYMP. ON USABLE PRIVACY & SECURITY (SOUPS) 199 [hereinafter Lin et al., 2014].

[62] *See* Lin et al., 2012, *supra* note 61.

[63] *See FAQ*, PRIVACYGRADE, *supra* note 34.

[64] *See id.*; Lin et al., 2014, *supra* note 61, at 199.

[65] *See FAQ*, PRIVACYGRADE, *supra* note 34.

[66] *Id.*

[67] *Id.*

[68] *Id.*

B. Privacy Labels and Icons

Other privacy indicators transform privacy policy content into labels or icons. For example, privacy "nutrition labels" synthesize policy text into a visual grid, much like the familiar nutrition labels that appear on food products across the United States. Similarly, the privacy icon system developed by Mozilla uses graphics to signal to users what privacy practices are stated or absent from a privacy policy. CommonTerms uses symbols to attempt to better explain complex data practices.

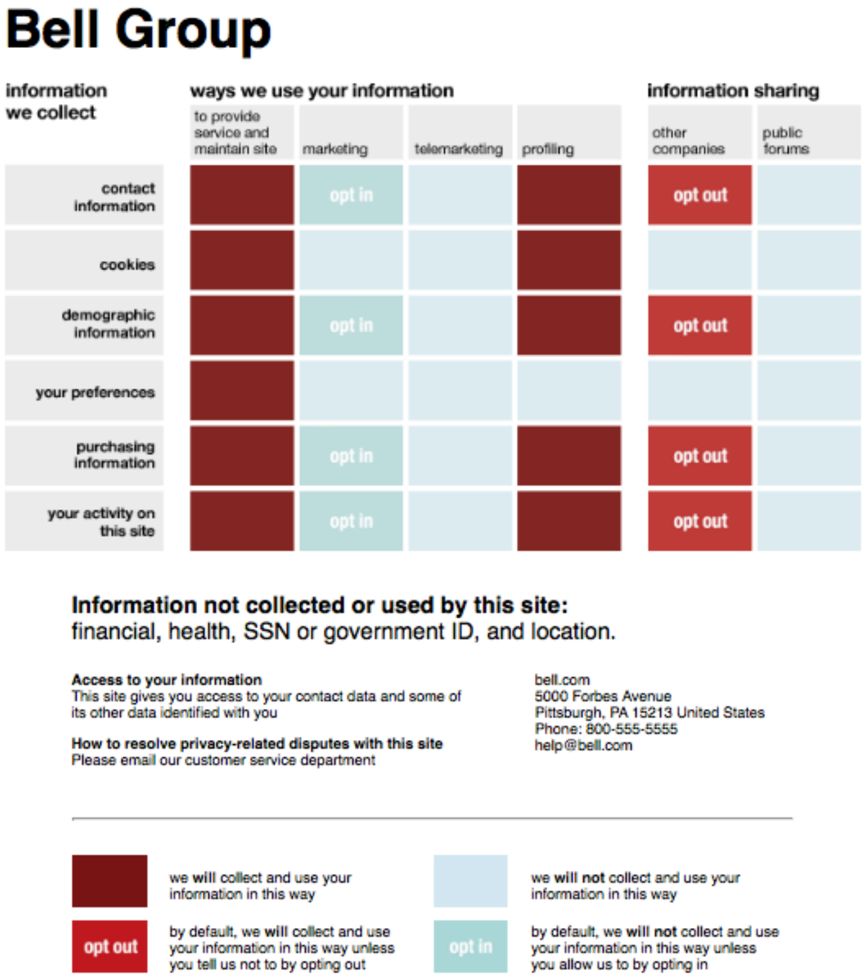
1. Privacy "Nutrition" Labels

Cranor and her research team developed privacy "nutrition labels" that seek to offer a "clear, uniform, single-page summary of a company's privacy policy" to resolve consumer concerns and assist in user comprehension.[69] The labels are presented in a standardized tabular format, shown at a consistent location, and use a color scheme to provide users with a high level picture of a privacy policy's substance.[70] Figure 1 is illustrative of Cranor and her team's work.

[69] Kelley et al., *supra* note 1, at 1.

[70] *See* Cranor, *supra* note 9, at 288.

Figure 1



Bell Group

information we collect	ways we use your information				information sharing	
	to provide service and maintain site	marketing	telemarketing	profiling	other companies	public forums
contact information	■	opt in	□	■	opt out	□
cookies	■	□	□	■	□	□
demographic information	■	opt in	□	■	opt out	□
your preferences	■	□	□	□	□	□
purchasing information	■	opt in	□	■	opt out	□
your activity on this site	■	opt in	□	■	opt out	□

Information not collected or used by this site:
financial, health, SSN or government ID, and location.

Access to your information
This site gives you access to your contact data and some of its other data identified with you

How to resolve privacy-related disputes with this site
Please email our customer service department

bell.com
5000 Forbes Avenue
Pittsburgh, PA 15213 United States
Phone: 800-555-5555
help@bell.com

■	we **will** collect and use your information in this way
□	we **will not** collect and use your information in this way
opt out	by default, we **will** collect and use your information in this way unless you tell us not to by opting out
opt in	by default, we **will not** collect and use your information in this way unless you allow us to by opting in

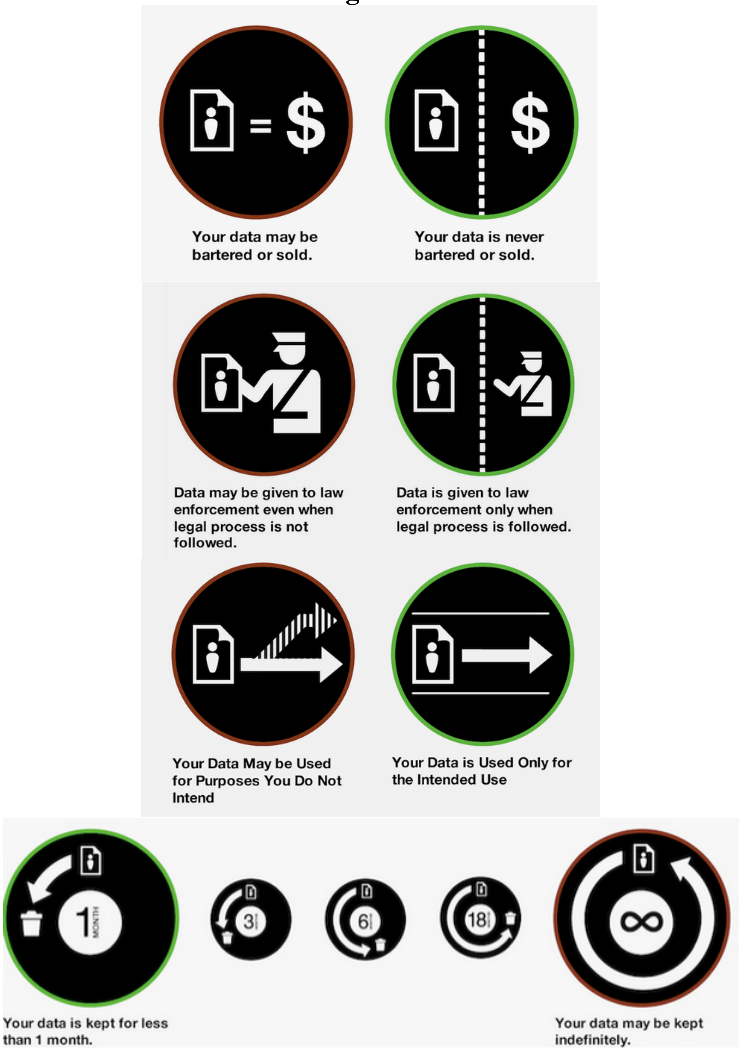
2. *Label and Icon Systems*

Aza Raskin led a working team that designed a machine-readable privacy icon system for Mozilla meant to "bolt on" to existing policies and offer website visitors an "iron-clad guarantee" about how a company treats user data.[71] The "bolt on" approach is based on recognizing that privacy policies can vary greatly from one another and that catch-all boilerplate may not work; thus, the emphasis is in using privacy icons to signal basic customer

[71] *See Privacy Icons*, MOZILLA WIKI, *supra* note 32; *see also* Cranor, *supra* note 9, at 294.

data usage. The team initially proposed ten icons, broken down into four categories, as shown in Figure 2.[72]

Figure 2


Your data may be bartered or sold.
Your data is never bartered or sold.
Data may be given to law enforcement even when legal process is not followed.
Data is given to law enforcement only when legal process is followed.
Your Data May be Used for Purposes You Do Not Intend
Your Data is Used Only for the Intended Use
1 MONTH
3
6
18
Your data is kept for less than 1 month.
Your data may be kept indefinitely.

[72] *See Privacy Icons*, MOZILLA WIKI, *supra* note 32.

The Mozilla team updated the icon designs in 2011 but has neither yet adopted the privacy icon system nor released any information concerning future development plans.[73]

CommonTerms is also an initiative intended to make online legal policies more accessible to consumers.[74] After finding that the creation of hundreds of unique symbols and icons representing different terms was impractical, CommonTerms morphed its original presentation into a drop-down menu that appears on the webpage after a user clicks on a "preview terms" button.[75] The drop-down features a short, human-readable, single-page standardized explanation of policies, each with accompanying symbols to help communicate complex privacy concepts to consumers.[76]

C. Privacy Certification Regimes and Seals

Privacy certifications and seals are a third category of privacy indicators. Businesses and data processors often rely on certification and seal programs to convey compliance with established legal or industry practices.[77] For example, TrustArc, formerly known as TRUSTe, offers privacy certifications. Established in 1997 and renamed in 2017, TrustArc is a for-profit company[78] that provides clients with privacy assessment audits and data security certifications.[79] The company offers certification of cross-border data transfers and compliance with laws and regulations such as the Children's Online Privacy Protection Act (COPPA) and the GDPR through certifications like "TRUSTe Enterprise Privacy," "TRUSTed Data Collection Certification," and "TRUSTe Downloads Certification."[80] TRUSTe also offers dispute resolution services for certified companies.[81]

To obtain a TRUSTe Enterprise Privacy Certification (EPC), participating companies must provide TrustArc Privacy Solutions Managers with access to their privacy and data practices for comparison against

[73] *See id. See generally Open Policy & Advocacy: Mozilla's Official Blog on Open Internet Policy Initiatives and Developments*, MOZILLA, https://blog.mozilla.org/netpoli cy/ [https://perma.cc/YCS5-LB5G].

[74] *See Towards Better Online Terms & Conditions*, COMMONTERMS, *supra* note 30.

[75] *See What We Did*, COMMONTERMS, http://commonterms.net/WhatWeDid.aspx [https://web.archive.org/web/20161021133341/http:/www.commonterms.net/WhatWeDid.aspx]; *see also* LANNERÖ, *supra* note 50; *Towards Better Online Terms & Conditions*, COMMONTERMS, *supra* note 30.

[76] *See What We Did*, COMMONTERMS, *supra* note 75.

[77] *See supra* notes 48–49 and accompanying text.

[78] *About TrustArc*, TRUSTARC, https://www.trustarc.com/about/ [https://perma.cc/CF8T-35D2].

[79] *Privacy Management Platform*, TRUSTARC, https://www.trustarc.com/products/privacy-platform/ [https://perma.cc/Z4SZ-45UP].

[80] *See TRUSTe Privacy Certifications*, TRUSTARC, https://www.trustarc.com/products/certifications/ [https://perma.cc/QL6R-N45U].

[81] *See Privacy Dispute Resolution*, TRUSTARC, https://www.trustarc.com/products/dispute-resolution-services/ [https://perma.cc/5AV2-DF8M].

TRUSTe's Enterprise Privacy Certification Standards (EPCS).[82] The standards are based on "the OECD Privacy Guidelines, the APEC Privacy Framework, the EU General Data Protection Regulation (GDPR), the U.S. Health Insurance Portability and Accountability Act (HIPAA), ISO 27001 International Standard for Information Security Management Systems and other global privacy laws and regulations."[83] After discovery of necessary information has concluded, a findings report is delivered, highlighting gaps, risks, and actionable recommendations which must be fulfilled to achieve compliance. The EPCS have also required that participating companies maintain and abide by a privacy statement subject to TRUSTe's approval.[84] This privacy statement must include comprehensive disclosures of the participating company's data collection, retention, and sharing practices.[85] Participating companies must also provide users with: opt-out privileges for data practices that are not in accordance with the stated policies, the ability to withdraw consent for the use of their data in internet-based advertising, and access to their personal data among other practices for responsible data use and management.[86] Whereas an EPC offers broad certification of a company's first and third party practices, TRUSTe Data Collection Certification, previously known as TRUSTed Data, pertains specifically to a company's third-party data sharing practices and use of online behavioral advertising.[87] Figure 3 below is an example of TRUSTe offerings based on its website as of March 31, 2016.[88]

[82] *See Enterprise Privacy Certification*, TRUSTARC, https://www.trustarc.com/products/enterprise-privacy-certification/ [https://perma.cc/SK9K-W3KS].

[83] *Id.*

[84] *See* TRUSTE, ENTERPRISE PRIVACY & DATA GOVERNANCE PRACTICES CERTIFICATION ASSESSMENT CRITERIA, https://www.TRUSTe.com/privacy-certification-standards/program-requirements/ [https://perma.cc/56X8-FDL4] (last updated Sept. 4, 2018).

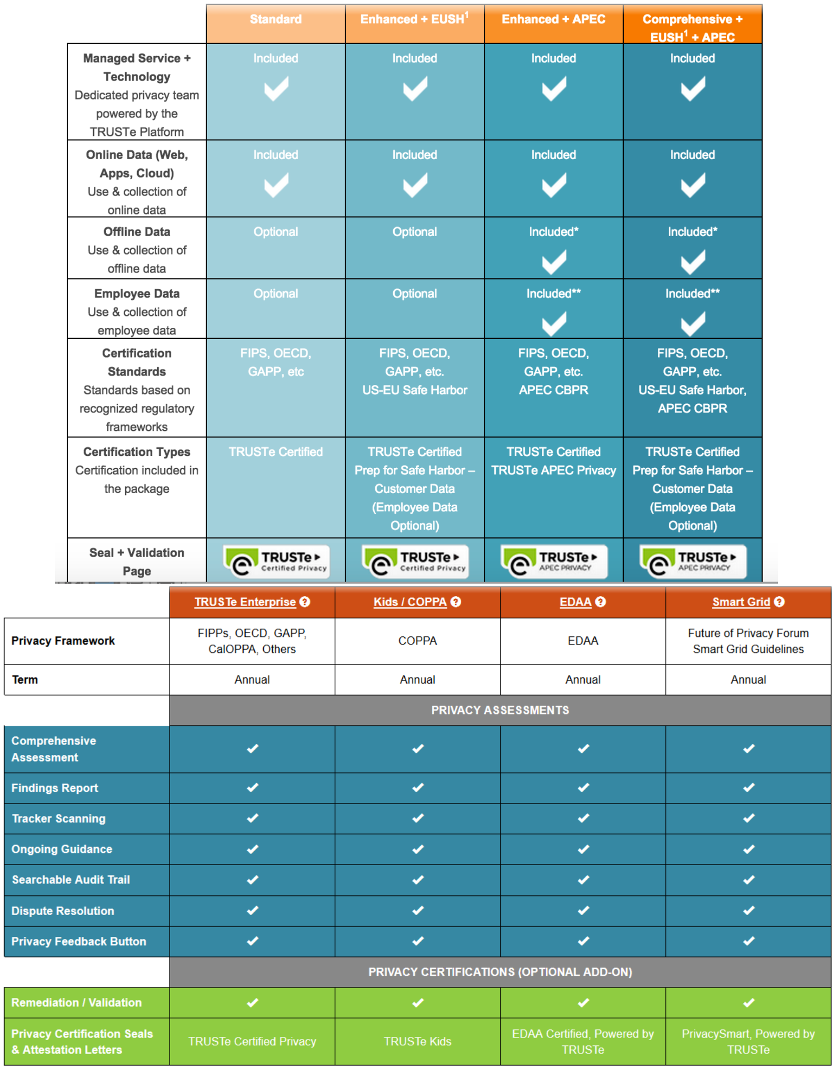
[85] *Id.*

[86] *Id.* TRUSTe does not explain what "access" means. *See id.*

[87] *See TRUSTe Data Collection Certification*, TRUSTARC, https://www.trustarc.com/products/data-certification/ [https://perma.cc/LCE2-ZAM3]; TRUSTE, TRUSTED DATA PROGRAM REQUIREMENTS (2016), https://www.truste.com/privacy-certification-standards/3rd-party-data-collection/ [https://perma.cc/T2N4-CXB9].

[88] *Privacy Assessments and Certifications*, TRUSTE, https://www.truste.com/business-products/dpm-services/ [https://perma.cc/QT37-HTFY].

Figure 3



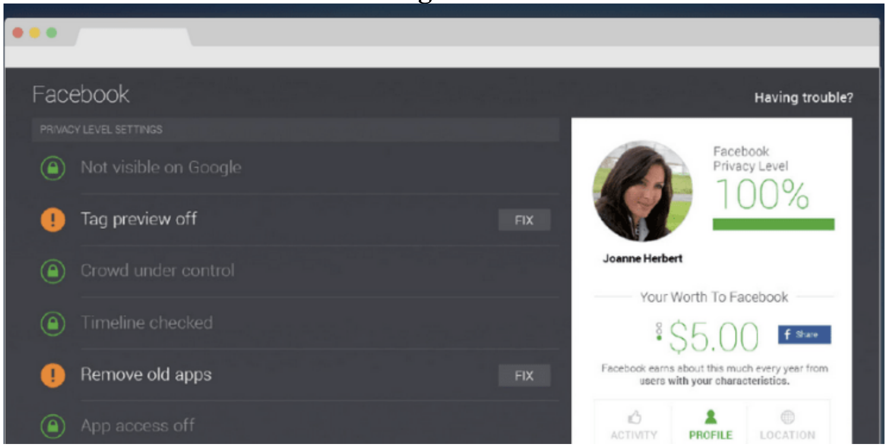
	Standard	Enhanced + EUSH[1]	Enhanced + APEC	Comprehensive + EUSH[1] + APEC
Managed Service + Technology Dedicated privacy team powered by the TRUSTe Platform	Included ✓	Included ✓	Included ✓	Included ✓
Online Data (Web, Apps, Cloud) Use & collection of online data	Included ✓	Included ✓	Included ✓	Included ✓
Offline Data Use & collection of offline data	Optional	Optional	Included* ✓	Included* ✓
Employee Data Use & collection of employee data	Optional	Optional	Included** ✓	Included** ✓
Certification Standards Standards based on recognized regulatory frameworks	FIPS, OECD, GAPP, etc	FIPS, OECD, GAPP, etc. US-EU Safe Harbor	FIPS, OECD, GAPP, etc. APEC CBPR	FIPS, OECD, GAPP, etc. US-EU Safe Harbor, APEC CBPR
Certification Types Certification included in the package	TRUSTe Certified	TRUSTe Certified Prep for Safe Harbor – Customer Data (Employee Data Optional)	TRUSTe Certified TRUSTe APEC Privacy	TRUSTe Certified Prep for Safe Harbor – Customer Data (Employee Data Optional)
Seal + Validation Page	TRUSTe Certified Privacy	TRUSTe Certified Privacy	TRUSTe APEC PRIVACY	TRUSTe APEC PRIVACY

	TRUSTe Enterprise	Kids / COPPA	EDAA	Smart Grid
Privacy Framework	FIPPs, OECD, GAPP, CalOPPA, Others	COPPA	EDAA	Future of Privacy Forum Smart Grid Guidelines
Term	Annual	Annual	Annual	Annual
	PRIVACY ASSESSMENTS			
Comprehensive Assessment	✓	✓	✓	✓
Findings Report	✓	✓	✓	✓
Tracker Scanning	✓	✓	✓	✓
Ongoing Guidance	✓	✓	✓	✓
Searchable Audit Trail	✓	✓	✓	✓
Dispute Resolution	✓	✓	✓	✓
Privacy Feedback Button	✓	✓	✓	✓
	PRIVACY CERTIFICATIONS (OPTIONAL ADD-ON)			
Remediation / Validation	✓	✓	✓	✓
Privacy Certification Seals & Attestation Letters	TRUSTe Certified Privacy	TRUSTe Kids	EDAA Certified, Powered by TRUSTe	PrivacySmart, Powered by TRUSTe

D. Privacy Dashboards

Privacy dashboards often take the form of web browser add-ons that offer privacy related information about the website a user is visiting at any given time. One example was AVG PrivacyFix, a mobile app and browser add-on that scanned a user's Facebook, Google, and LinkedIn privacy settings, highlighting settings that affected the user's level of vulnerability to data-permissive practices.[89] For each of these settings, the user was shown the pros and cons of maintaining or changing their setting, allowing the user to select his or her preferences manually.[90] PrivacyFix also showed which sites were tracking a user's online activities.[91] The PrivacyFix mobile app displayed a user's "privacy level," which increased each time the user reviewed a privacy setting the app had highlighted.[92] Below in Figure 4 is an example of the PrivacyFix dashboard[93]:

Figure 4



Facebook

Having trouble?

PRIVACY LEVEL SETTINGS

- Not visible on Google
- Tag preview off — FIX
- Crowd under control
- Timeline checked
- Remove old apps — FIX
- App access off

Facebook Privacy Level 100%

Joanne Herbert

Your Worth To Facebook

$5.00

Facebook earns about this much every year from users with your characteristics.

Similarly, Ghostery offers a browser extension and mobile app that help users see how they are tracked online across websites by otherwise invisible webpage-embedded trackers.[94] The service offers users the option to control which of these trackers to either block or permit.[95] Ghostery displays this information in a pop-up bubble or control pane above the webpage that a user is visiting.[96]

Most recently, European Commission-funded Online Privacy Enforcement, Rights Assurance and Optimization project (OPERANDO)

[89] *See FAQ*, PRIVACYFIX.COM, http://www.priv acyfix.com/start/faq [https://perma.cc/W6ZJ-R9U4]. The AVG PrivacyFix program has been terminated as of April 2016 and has been replaced by AVG Web Tune Up. *See AVG Support Community: AVG PrivacyFix Replacement?*, AVG, https://support.avg.com/answers?id=906b0000000cKPqAAM [https://perma.cc/R7DV-GWCR].

[90] *See* FAQ, PRIVACYFIX.COM, *supra* note 89.

[91] *Id.*

[92] *Id.*

[93] *PrivacyFix: Online Privacy Dashboard for Social Networks*, LEGAL DESIGN LAB, http://www.legaltechdesign.com/communication-design/privacyfix-online-privacy-dashboard-for-social-networks/ [https://perma.cc/NDB6-7Z3F].

[94] *See Welcome to Ghostery*, GHOSTERY, https://extension.ghostery.com/intro#welcome [https://perma.cc/27SJ-M7Z2] (introductory tour on Ghostery's website).

[95] *Id.*

[96] *Id.*

has developed PlusPrivacy, a unified privacy settings dashboard allowing users to manage data sharing, monetize their information, set up email aliases, and block trackers all from one place.[97] The code is open source, available on GitHub.[98]

III. OBSTACLES TO MEANINGFUL PRIVACY INDICATORS

An analysis of privacy indicator initiatives reveals specific deficiencies and obstacles that hamper their overall effectiveness and widespread adoption. For one, the lack of governmental guidance and developer consensus has led to a stratification of efforts detrimental to building common ground. Second, the ensuing non-standardized selection and weighting of scoring criteria results in incomparable and sometimes defective rating schemes. Some initiatives, like ToS;DR, in fact, end up producing indicators that may be deemed inconsistent and arbitrary. Third, inaccurate interpretation of privacy policy statements—and of the criteria designed to rate those statements—makes it difficult to devise indicators that are meaningful. Fourth, inconsistent rating agent reliability has dampened the trust indicators are supposed to instill with consumers. This section explores each challenge in turn.

A. Lack of Standardization

Lack of standardization is a serious obstacle to the development of meaningful privacy indicators. Even when it exists, public guidance remains limited. In the United States, even though the FTC has encouraged the use of icons or indicators, it has not issued any formal standards or guidelines for what indicators should require or a standardized baseline for what privacy ratings should be.[99] The same applies to the European Union's GDPR. While the regulation empowers the European Commission to "adopt delegated acts . . . for the purpose of determining the information to be presented by the icons and the procedures for providing standardised icons,"[100] no such measures have been taken at the time of writing. The lack

[97] *See* PLUSPRIVACY, https://plusprivacy.com/ [https://perma.cc/GT7Q-D4V9].

[98] *See OPERANDO H2020/PlusPrivacy*, GITHUB, https://github.com/OPERANDOH2020/PlusPrivacy [https://perma.cc/WBQ4-AG6G].

[99] The Commission has recommended that app trade associations explore developing standardized icons, and has provided an example of a mobile device icon that notifies users when an app is collecting data and discloses the types of information collected and its purpose. *See* FED. TRADE COMM'N, MOBILE PRIVACY, *supra* note 11, at 25. Additionally, the FTC has required the use of icons in consent orders: for example, as part of its settlement terms with Aspen Way Enterprises, the Commission ordered the company to display "a clear and prominent icon" on the device every time Aspen used any geophysical location tracking technology. Aspen Way Enters., Inc., 155 F.T.C. 483, 494 (2013) (consent order).

[100] GDPR, *supra* note 21, art. 12(8), at 40.

of any formal guidelines has resulted in a densely populated landscape of privacy indicator attempts.[101] Many of these rating schemes are limited to a particular application such as mobile apps,[102] finance,[103] entertainment,[104] advertising,[105] and even specific websites.[106] This reality obscures different schemes' visibility and makes it difficult to achieve uniformity in the marketplace.

A lack of standardization has also resulted in weak incentives for consumers and industry alike to adopt and invest in a privacy indicator system. Non-uniformity is problematic for consumers where a proliferation of competing icons, grading schemes, and privacy policies can make it difficult for the consumer to recognize, meaningfully pick, and rely on a given indicator.[107] For example, an icon system with many complex designs has a steep learning curve. However, companies with sophisticated data practices may need many different intricate icons to achieve meaningful consumer notice of data practices with granularity. For businesses, there is little incentive to adopt a privacy indicator that might misrepresent their privacy statements or accurately represent practices that consumers may find unfavorable. [108] This problem was acknowledged during the development of Mozilla's privacy icon system; at one point, the developers considered the solution of "automatically display[ing] the icons with the poorest guarantees" for companies that did not adopt the system as a means of incentivizing widespread icon adoption. [109] Furthermore, when a company wishes to take market advantage of its strong privacy practices, it

[101] *See, e.g.*, LANNERÖ, *supra* note 50; *see also supra* Part 0.

[102] *See, e.g.*, *ESRB Privacy Certified Introduces New Services for Mobile Apps*, MARKETWIRED (June 25, 2013, 10:00 AM), http://www.marketwired.com/press-release/esrb-privacy-certified-introduces-new-services-for-mobile-apps-1805567.htm [https://perma.cc/STC8-W5NP]; *FAQ*, PRIVACYGRADE, *supra* note 34.

[103] *See, e.g.*, *Overview of WebTrust Services*, WEBTRUST, http://www.webtrust.org/item64428.aspx [https://perma.cc/HF2X-VBUL].

[104] *See, e.g.*, *ESRB Privacy Certified*, ENTM'T SOFTWARE RATING BD., http://www.esrb.org/privacy/ [https://perma.cc/MLF9-WFMT].

[105] *See, e.g.*, DIG. ADVERT. ALL. (DAA) SELF-REGULATORY PROGRAM, http://www.aboutads.info/ [https://perma.cc/3A8F-MWWA].

[106] AVG's Privacy Dashboard was limited to the analysis of Google, Facebook and LinkedIn's privacy policies. *See supra* note 89 and accompanying text.

[107] *See* FED. TRADE COMM'N, MOBILE PRIVACY, *supra* note 11, at 27.

[108] This factor, to a certain extent, led to the failure of the Platform for Privacy Preferences (P3P system). *See* Cranor, *supra* note 9, at 274–75. To some, P3P's failure is the proof that self-regulation is bound to fail because in the absence of enforcement, businesses lack incentive to "emphasize the potentially unsavory collection of personal data on the Web." William McGeveran, Note, *Programmed Privacy Promises: P3P and Web Privacy Law*, 76 N.Y.U. L. REV. 1812, 1846 (2001); *see also* Neil Weinstock Netanel, *Cyberspace Self-Governance: A Skeptical View from Democratic Theory*, 88 CALIF. L. REV. 395, 478–80 (2000).

[109] Declan McCullagh, *Mozilla Weighs Privacy Warnings for Web Pages*, CNET (Feb. 2, 2010), https://www.cnet.com/news/mozilla-weighs-privacy-warnings-for-web-pages/ [https://perma.cc/3NUR-ATKA].

often pays to obtain a certification or seal.[110] Therefore, a successful privacy indicator scheme must strike the appropriate balance between social and economic incentives,[111] and there is unresolved debate as to what this balance is without standardization.

B. Scoring Criteria Deficiencies

Deficiencies in the scoring criteria that undergird privacy indicators obstruct the indicators' success. For example, Enonymous displayed privacy ratings ranging from one to four stars, but it only existed for two years.[112] What does it mean to have only one star and not two stars? What is the basis for the four-star system? Two problems in particular stand out—one arising from the selection of the scoring criteria used to inform the indicator, and the second regarding the relative weighing of this criteria in calculating a grade, rank, or score.

1. Selection of Grading Criteria

One issue involves the selection of the criteria on which a privacy indicator's rating is based. A lack of breadth or depth in a given indicator's grading criteria will undermine its value to the consumer.[113] For example, are privacy policy statements regarding data collection, sharing, use, and retention *all* included within the scoring criteria? Which ones are included, which are omitted, and why? In the absence of a standardized process for choosing relevant criteria, the selected criteria can differ significantly from one indicator to another as well as between different ratings by the same indicator if based on different user expectations or preferences. Incomplete criteria may result in an indicator providing potentially deceptive or misunderstood information.

A good example is ToS;DR. Although its process for scoring topics is stated to be transparent and peer-reviewed, the platform does not articulate a procedure for debating and assigning a score: anyone wishing to collaborate may simply propose a score on its website based on contributed privacy policy elements;[114] ToS;DR team members can then choose

[110] *See, e.g.*, *Get Accredited*, BETTER BUS. BUREAU, https://www.bbb.org/en/us/become-accredited (last visited July 11, 2018).

[111] *See* Cranor, *supra* note 9, at 305–07.

[112] *See infra* Appendix.

[113] The selection criteria for Mozilla's privacy icons are very limited and focus only on commercial data sale, access to data by law enforcement, whether data is used for an intended purpose, and data retention. *See Privacy Icons*, MOZILLA WIKI, *supra* note 32; *see also* Cranor, *supra* note 9, at 294.

[114] *See supra* notes 54–55 and accompanying text.

whether or not to display the score on the ratings website.[115] Submission criteria and selection methodology, however, remain very broad.[116] Thus, a score may be based on subjectivity or an incomplete evaluation of a privacy policy's stated data practices.[117] Inconsistent contributor participation in ToS;DR threads may also lead to inconsistencies, some having more than ten replies while others elicit none.[118] Additionally, ToS;DR explains neither what constitutes an adequate number of badges for a classification[119] nor what score is required to be placed within a certain class.[120] As a result, privacy content may not be scored uniformly, and ToS;DR scores may be incomparable with one another.[121] If a ToS;DR score is based on an incomplete evaluation or is otherwise not scored with uniformity, the score becomes less meaningful and potentially confusing for users.

Another example is PrivacyGrade.org, which assigns grades based upon the disparity between user expectations as to what are appropriate data practices and an application's actual practices.[122] This grading criteria may be too limited. Many actual data practices may not be discernable with granularity by external research methods or from review of privacy policy language. Also, users' expectations as to reasonable data practices will vary and may not be amply informed—either because a user does not conceive that certain data activities are possible and ongoing or because a user has expectations that are too high in light of peer expectations or industry norms. The success of any privacy indicator requires the development of, and adherence to, an objectively-sound, standardized list of clearly defined scoring criteria.

[115] *See Ratings*, TOS;DR, *supra* note 58; *see also supra* note 55.

[116] *See Get Involved*, TOS;DR, https://tosdr.org/get-involved.html [https://perma.cc/SZN5-9W7E].

[117] As another example, Enonymous's highest ranking was awarded to "sites that do not contact you without your permission and do not share your personal information with anyone at all," as determined by reviewers who spent "about 10 minutes" reviewing a site. *See Odd Privacy Ratings Exposed*, WIRED (Apr. 12, 2000, 3:00 AM), http://archive.wired.com/politics/law/news/2000/04/35587?currentPa ge=all [https://perma.cc/9MDS-LDN8].

[118] *See supra* note 55.

[119] For example, DuckDuckGo is rated a Class A service, despite having only two topic reviews, while Facebook has no classification yet, although ToS;DR lists fourteen separate entries evaluating nine topics. *See Ratings*, TOS;DR, *supra* note 58. DuckDuckGo is also listed as one of two companies that have donated to the ToS;DR organization. *See Thank You!*, TOS;DR, https://tosdr.org/thanks.html [https ://perma.cc/3DWR-PNVE].

[120] *See Classification*, TOS;DR, *supra* note 31.

[121] *See Topics*, TOS;DR, *supra* note 54 (cautioning that "the same clause can have different scores depending on the context of the services it applies to").

[122] *See* Lin et al., 2012, *supra* note 61; Lin et al., 2014, *supra* note 61, at 2.

2. Weighting of Grading Criteria

The second issue is how to determine the relative weight afforded to each of the scoring criteria in the calculation of a grade, rating, or score or in determining how to label or certify for privacy value. For example, should privacy policy statements about collection practices and sharing practices be weighted equally? Should all practices within a category (*e.g.*, collection, sharing, or selling) be equally weighted, or do some practices within a particular category merit more or less weight than others? Some topics, like sharing user data with law enforcement officials or selling it to brokers may merit greater weighting than other more innocuous practices. Likewise, are all data points weighted equally? Is location data weighted the same as medical data or financial data? If weighted differently, what is the basis for the different weighting?

Thus, a rating system that assigns each scoring criterion equal weight can produce ratings that are skewed or misleading. If all scoring criteria are afforded equal weight, a policy with one very troubling practice would still rate highly overall despite the poorly rated criterion. In essence, the preponderance of well-rated criteria would dilute the poorly-rated criterion's effect on an overall rating. Such an outcome is problematic—especially if the poorly-rated criterion is objectively egregious or subjectively objectionable to the user interpreting and relying upon the rating system. In contrast, the diminishing effect described above would be mitigated in a rating system that weighs scoring criteria according to their respective importance.

However, determining the proper weights to be assigned to each scoring criterion is an issue. Assigning weights to scoring criteria can be subjective or, similarly, fail to account for the contextual complexity of data practices. Even for developers of indicators with particular expertise, the contextual specificity of data practices will make it very difficult to develop a justifiable weighting. Some schemes may base a metric on a subjective standard like the difference between consumer expectations and a website's actual practices, while others will rely on a more objective standard like website policy conformity to a set of best practices.[123] The bottom line is

[123] PrivacyGrade.org's website states that its grades denote levels of "privacy sensitiv[ity]." *See FAQ*, PRIVACYGRADE, *supra* note 34. However, PrivacyGrade.org does not define "privacy sensitiv[ity]," and its grades are derived from the subjective metric of user expectation as opposed to a comparison of policies against an objective benchmark for privacy sensitivity. *Id.* Similarly, Privacy Bird allows users to generally select a low, medium or high level privacy threshold, then informs the user whether a website's privacy practices exceed or fall below that threshold. *See Privacy Preferences*, PRIVACY BIRD, http://www.privacybird.org/tour/1_3_beta/privacypreferences.html [https://perma.cc/FF9K-ZWTD]; *Privacy Bird Tour*, PRIVACY BIRD, http://www.privacybird.org/tour/1_3_beta/tour.html [https://perma.cc/F7GA-J5C6]. Disconnect's Privacy Icon plug-in represents whether the website's privacy policy discloses that the data it collects is used in ways other than a user would reasonably expect

that a subjective grading scheme will not be easily comparable for the common consumer, thus limiting its utility. Therefore, privacy indicator systems need some common, objective basis for weighing scoring criteria.

C. Interpretation Issues

Interpretive issues also obstruct the success of privacy indicators. By their nature, privacy indicators must translate broad privacy policy language representing intricate and nuanced data practices into simple, clear, concise, and accurate summaries encapsulated in a final visual representation—an inherently challenging process. Accurately interpreting privacy statements is a complex and problematic issue when developing and deploying privacy indicators.[124]

Several interpretive difficulties exist. First, privacy indicators abandon a holistic approach to privacy policy interpretation. Second, privacy indicators may not account for vagueness, ambiguity, or silence in policies. Third, the interpretations of human annotators whose efforts form the baseline evaluation standard for the analytic tools used to facilitate privacy indicators can be inconsistent or inaccurate.

1. Non-holistic Interpretive Approach

It is well established in law that a document must be interpreted as a whole—not in isolated parts—and that the interpretation must give effect to all the document's terms in a way that consistently comports with the document's general purpose.[125] However, the automated tools and other techniques privacy rating schemes often use to interpret privacy policy content and assign indicators abandon such a holistic interpretive approach in favor of more granular textual analysis. For example, ToS;DR conducts its initial privacy policy analyses based on Google group users' discussions

given the site's expected use, without clarity as to objective establishment of the reasonable user's data use expectations. *See* DISCONNECT, https://disconnect.me/ [https://perma.cc/R23R-GVNH].

[124] For example, one study of icons designed to reflect behavioral advertising practices found that the representations were confusing and concluded that it was unclear how well online behavioral advertising icons could actually communicate with users. *See* Hastak & Culnan, *supra* note 3, at 3.

[125] *See, e.g.*, Alta Berkeley VI C.V. v. Omneon, Inc., 41 A.3d 381, 385–86 (Del. 2012) (quoting Elliott Assocs., L.P. v. Avatex Corp., 715 A.2d 843, 854 (Del. 1998)) ("[I]t is well established that a court interpreting any contractual provision . . . must give effect to all terms of the instrument, must read the instrument as a whole, and, if possible, reconcile all the provisions of the instrument."); JA Apparel Corp. v. Abboud, 568 F.3d 390, 397 (2d Cir. 2009) (quoting Kass v. Kass, 91 N.Y.2d 554, 566 (1998)) (second alteration in original) ("[T]he court is to consider its '[p]articular words' not in isolation 'but in light of the obligation as a whole and the intention of the parties manifested thereby.'"); Int'l Klafter Co. v. Cont'l Cas. Co., 869 F.2d 96, 99 (2d Cir. 1989) (quoting Tougher Heating & Plumbing Co. v. New York, 423 N.Y.S.2d 289, 290–91 (N.Y. App. Div. 1979)) ("[T]he court must look to 'all corners of the document' rather than view sentences or clauses in isolation . . . .").

of short policy segments.[126] This approach risks overlooking important contextual clues that might appear elsewhere in a policy. Similarly, the approach can result in interpreters' failing to observe ambiguities, vagueness, or inconsistencies present in the policy.[127] This method of isolating and interpreting policy statements out of the context of the entire policy contrasts with legal maxims of contractual interpretation, and ultimately casts doubt on the validity of any rating resulting from it.

2. Ambiguity, Vagueness, and Silence in Privacy Statements

Privacy policy language is often ambiguous, vague, or silent about a service's data practices, which makes accurate interpretation difficult and often impossible.[128] These characteristics obstruct the meaningfulness of privacy indicators' ratings because, often, the automated tools and related techniques privacy rating schemes use to interpret privacy policy content and assign indicators do not account for the contextual complexities that ambiguity, vagueness, and silence create. Indeed, privacy policy drafters frequently use flexible language. The numerous and intricate ways that companies use data make it difficult to accurately describe all information practices in a concise privacy statement.[129] Thus, policy drafters often generalize complex information practices.[130] This pragmatic approach enables companies to alter particular information practices in the future without necessitating any policy revisions.[131] Further, the use of general language is prudent for avoiding legal liability: a specification of precise data practices may inadvertently rise to the level of deception in the event that the specified practices change, as the privacy policy would then be inaccurate.[132]

Policy drafters use modal language (*e.g.*, "may" or "might"), conditional terms (*e.g.*, "if") generalizations (*e.g.*, "usually"), and open ended

[126] *See supra* notes 54–55 and accompanying text.

[127] *See infra* Parts IV.B.2 & 3.

[128] Joel R. Reidenberg et al., *Ambiguity in Privacy Policies and the Impact of Regulation*, 45 J. LEGAL STUD. S163, S163 (2016).

[129] *See* Robert H. Sloan & Richard Warner, *Beyond Notice and Choice: Privacy, Norms, and Consent*, 14 J. HIGH TECH. L. 370, 390–98 (2014); Mark MacCarthy, *New Directions in Privacy: Disclosure, Unfairness and Externalities*, 6 I/S J.L. & POL'Y FOR INFO. SOC'Y 425, 436–37 (2011); Cranor, *supra* note 9, at 274 ("Privacy policies for the first-party websites that users interact with are difficult enough for users to understand, but when third-party sites enter the mix, the notion of effective privacy notice becomes completely untenable.").

[130] *See* Reidenberg, *supra* note 128, at S170.

[131] *See id.*

[132] FTC policy considers a trade practice to be deceptive when it involves a "misrepresentation, omission or other practice that misleads the consumer acting reasonably in the circumstances, to the consumer's detriment." *See* Letter from James C. Miller III, Chairman, FTC, to Hon. John D. Dingell, Chairman, House Comm. on Energy & Commerce (Oct. 14, 1983), *reprinted in* Cliffdale Assocs., Inc., 103 F.T.C. 110, 174, 183 (1984) (decision & order).

quantifiers (*e.g.*, "some" or "many") to describe data practices.[133] Such terms create the opportunity for multiple possible outcomes for the data practice they describe. These types of terms also allow for lists to be non-exhaustive and for large permissive space through silence. This presents a significant challenge for privacy indicators' interpretive tools, as the ambiguous and vague nature of such terms frustrates a tool's ability to categorize a statement as a definite, binary signifier that a service either does or does not engage in a particular data practice. Similarly, policy silence about a particular data practice blemishes the efforts of interpretive tools that fail to account for a legal default that treats silence as permissive, not prohibitive, with respect to a certain data practice.

3. *Annotator Consistency*

Privacy indicators must rely on human input at some level. Often, automated or semi-automated interpretive tools used to rate privacy policies rely on human policy annotations as a baseline evaluation standard.[134] Whether policies are rated based on human evaluation alone[135] or by tools that automatically interpret policy language, inconsistencies can result from human influence. Any error or unresolved inconsistency in this foundation carries through to the indicator's final result.

Research shows that there are discrepancies in user comprehension of key terms in privacy policies.[136] Both knowledgeable annotators—graduate students studying law and/or computer science—and crowd workers sometimes have had difficulty interpreting the language used in privacy policies.[137] Expert annotators—specialists in the fields of law, privacy, and natural language processing—also disagreed on specific terms.[138] These discrepancies show that knowledgeable users and crowd workers "misapprehend websites' data practices" and that privacy policy language generates disagreement even among expert readers.[139] As put succinctly by linguist Steven Pinker, "[w]e are verbivores, a species that lives on words,

[133] *See* Reidenberg, *supra* note 128, at S167–69.

[134] *See, e.g.*, Sushain K. Cherivirala et al., *Visualization and Interactive Exploration of Data Practices in Privacy Policies*, 2016 PROC. 12TH SYMP. ON USABLE PRIVACY & SECURITY (SOUPS) POSTER SESSION 3 (2016), https://www.usenix.org/sites/default/files/soups16poster25-cherivirala.pdf [https://perma.cc/35ZT-HAK4] (describing the annotation method for a privacy policy corpus that will be used to develop a privacy-oriented browser plugin).

[135] *See, e.g.*, *Classification*, TOS;DR, *supra* note 31.

[136] *See generally* Joel R. Reidenberg et al., *Disagreeable Privacy Policies: Mismatches Between Meaning and Users' Understanding*, 30 BERKELEY TECH. L.J. 39 (2015) [hereinafter *Disagreeable Privacy Policies*].

[137] *Id.* at 87.

[138] *Id.* at 62–83.

[139] *Id.* at 87.

and the meaning and use of language are bound to be among the major things we ponder, share, and dispute."[140]

Often, such discrepancies result from difficulties interpreting ambiguous or vague language in policies. [141] Alternatively, annotators may misunderstand how certain technologies operate, and consequently interpret policy statements about those technologies inaccurately. One example of this is when a policy informs users that they may delete their accounts: users who lack sufficient understanding may not realize that some websites store data and information associated with a user's account even after the user has deleted his or her account with an online service.[142] Another example is where a website uses cookies and users are not knowledgeable about the extent to which cookies might collect or share their information.[143] In either example, annotators risk interpreting related privacy policy statements differently and incorrectly. Where human interpreters are likely to miscomprehend policy language, automated analysis tools are likely to also fail in these areas. These inaccurate interpretations could, in turn, lead to an inaccurate rating by the privacy indicator relying on those interpretations as an evaluation baseline.

Furthermore, even if privacy language is clear and users have complete knowledge of every technical nuance, reasonable minds may still differ over topics like the significance of the various data practices described in privacy policies. In many cases, the context in which data is collected or used may be more meaningful than the volume and nature of that collection or sharing.[144] However, context is often difficult to glean when the complex data practices represented in privacy policies are synthesized into simplified indicators such as labels or icons. This is especially true for schemes where the condensing is not limited to the final indicator but which require additionally that various "data categories" be "collapsed together [into] similar data categories, purposes, and recipients" (*e.g.*, physical and online

[140] STEVEN PINKER, THE STUFF OF THOUGHT: LANGUAGE AS A WINDOW INTO HUMAN NATURE 24 (2007).

[141] *See generally Disagreeable Privacy Policies*, *supra* note 136; Reidenberg, *supra* note 128. *See also infra* Part IV.B.2.

[142] *See, e.g.*, *Securely Delete Files and Clean Diskspace*, TAILS, https://tails.boum.org/doc/encryption_and_privacy/secure_deletion/index.en.html [https://perma.cc/79B5-FNAT] (acknowledging that the company's operating systems only "remove the file's entry from the file system directory, because this requires less work and is therefore faster" and that "[t]he contents of the file—the actual data—remain on the storage medium . . . until the operating system reuses the space for new data.").

[143] *See Disagreeable Privacy Policies*, *supra* note 136, at 75 n.97.

[144] Professor Helen Nissenbaum refers to this notion as "contextual integrity." *See* Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 119 (2004) ("Contextual integrity ties adequate protection for privacy to norms of specific contexts, demanding that information gathering and dissemination be appropriate to that context and obey the governing norms of distribution within it.").

contact information were merged into a single "contact information" row on the indicator).[145]

Inaccurate interpretation may also arise when the surveys, questions, or similar prompts used to produce the human annotations are themselves ambiguous or vague.[146] When prompts are unclear or not objective, annotators may interpret policy statements incorrectly when they would have made correct interpretations but for the flawed prompts. Prompts may introduce a first layer of ambiguity into the analysis from the start, with the potential for a second layer in the rating indicator output once unclear policy language is introduced. Developers of privacy tools should be mindful of this dual ambiguity problem—ambiguity in tasks of the annotation tool and policy language—and reduce ambiguity in questions presented to annotators.

D. Rating Agent Reliability

Meaningful privacy indicators are threatened when rating agents are unreliable. One type of unreliability arises when the rating agent has questionable integrity. For example, in 2014, the FTC fined TRUSTe for failing to re-certify participating companies on a yearly basis in violation of its own policies, and also for representing itself as a not-for-profit organization when such was no longer the case.[147] On April 6, 2017, TRUSTe entered a $100,000 settlement with New York's Attorney General over flaws in its child privacy certification program.[148] Similarly,

[145] Cranor, *supra* note 9, at 290.

[146] *See, e.g.*, *Disagreeable Privacy Policies*, *supra* note 136, at 56–61 (describing the privacy policy survey and annotations used in the study). This issue mirrors critiques of Professor Alan Westin's renowned privacy surveys that question both the assumptions underlying his privacy segmentation and the varying of criteria over time to develop his framework. *See* PONNURANGAM KUMARAGURU & LORRIE FAITH CRANOR, PRIVACY INDEXES: A SURVEY OF WESTIN'S STUDIES 3–4, 16, 19–20 (2005), https://www.cs.cmu.edu/~ponguru/CMU-ISRI-05-138.pdf [https://perma.cc/D26C-H39N]; *see also* Chris Jay Hoofnagle & Jennifer M. Urban, *Alan Westin's Privacy* Homo Economicus, 49 WAKE FOREST L. REV. 261 (2014).

[147] *See* True Ultimate Standards Everywhere, Inc., 159 F.T.C. 970, 988–89 (2015) (final determination); Edward Wyatt*, F.T.C. Penalizes TRUSTe, a Web Privacy Certification Company*, N.Y. TIMES (Nov. 17, 2014), http://www.nytimes.com/2014/11/18/technology/ftc-penalizes-truste-a-web-privacy-certification-company.html?_r=0 [https://perma.cc/YR4W-E5MD]; *see also* Nora J. Rifon et al., *Your Privacy Is Sealed: Effects of Web Privacy Seals on Trust and Personal Disclosures*, 39 J. CONSUMER AFF. 339, 342–43 (2005) ("TRUSTe was embarrassed to find that it had violated its own standards by using (unwittingly, it claimed) a third party to track identifiable information on its own site. Two TRUSTe seal holders were found forwarding personal information to a marketing company, and while TRUSTe vowed to investigate and the transfer was eventually terminated, the authority never published the result of its investigation. TRUSTe also failed to pursue complaints against Microsoft and RealNetworks on the premise that software glitches had inadvertently caused the breaches. Both authorities have been criticized for granting seals to companies that were under investigation by the FTC (GeoCities in the case of TRUSTe, Equifax in the case of BBBOnline).").

[148] N.Y. Attorney Gen.'s Press Office, *A.G. Schneiderman Announces $100,000 Settlement with TRUSTe over Flawed Privacy Certification Program for Popular Children's Websites*, N.Y. ATTORNEY

Enonymous faced criticism for collecting more of users' sensitive information than was necessary, thereby rousing concern that the data could be "sold" or "corrupted."[149]

A rating agent may also threaten its reliability when it does not remain faithful to its scoring criteria. For example, concerns arose that criteria used by Enonymous to grade websites was extremely vague and not applied uniformly.[150] In addition, one may view the privacy dashboards offered by Google and Microsoft, for example, as unreliable if deemed constructed and controlled by a biased self-regulating entity.[151]

The lack of reliability also arises if a rating agent's sustainability is not certain. Privacy indicators are often dependent on particular individuals or organizations. Thus, institutional breakdowns can halt success of an effort to develop and maintain a privacy indicator. For example, the Mozilla icon project stalled when its initiator left the company to found another.[152] The Mozilla team updated the icon designs in 2011, but the project's official webpage indicates no progress since then.[153] The success of a privacy indicator scheme requires continued attention and support of individuals and institutions.

Similarly, because many privacy indicators are dependent on human effort, a rating agent's inability to put forth necessary resources jeopardizes its continued success. For example, Enonymous's team of site raters managed to grade over 30,000 policies;[154] yet as of June 2017, the number of websites online was estimated at over 1.7 billion.[155] Even efforts such as

GEN. (Apr. 6, 2017), https://ag.ny.gov/press-release/ag-schneiderman-announces-100000-settlement-truste-over-flawed-privacy-certification [https://perma.cc/Q82H-RBHH]. A study by Professor Benjamin Edelman published in 2009 found that TRUSTe's lack of substantial verification of certification recipients gave rise to a process of adverse selection where participating websites were twice as likely to be untrustworthy as non-certified websites. Benjamin Edelman, *Adverse Selection in Online "Trust" Certifications*, 2009 PROC. 11TH INT'L CONF. ON ELECTRONIC COM. 205, http://www.benedelman.org/publications/advsel-trust.pdf [https://perma.cc/B94H-G7QQ]. The same study found that the Better Business Bureau's stricter OnLine Privacy Seal had three times less untrustworthy certified websites than non-certified ones. *Id.* at 210.

[149] To access privacy ratings, Enonymous required users to provide information including their "name, date of birth, shipping and billing addresses, e-mail address, phone number, credit card number and preferred method of contact." *See* Catherine Greenman, *Efforts to Keep the Web from Getting Too Personal*, N.Y. TIMES (Apr. 27, 2000), https://partners.nytimes.com/library/tech/00/04/circuits/articles/27priv.html [https://perma.cc/4RUT-T P28].

[150] *See Odd Privacy Ratings Exposed*, *supra* note 117. According to an article in *Wired*, websites owned by the same company having identical policies were assigned a different number of stars. *See id.*

[151] *See infra* Appendix.

[152] *See, e.g.*, Tim Chambers, *Part Three: Who Owns the Digital You?*, HUFFINGTON POST (Apr. 8, 2011, 2:58 PM), http://www.huffingtonpost.com/tim-chambers/part-three-who-owns-the-d_b_846385.html [https://perma.cc/ 9R6R-43RF].

[153] *See Privacy Icons*, MOZILLA WIKI, *supra* note 32.

[154] *See* Greenman, *supra* note 149.

[155] *See Total Number of Websites*, INTERNET LIVE STATS, http://www.internetlivestats.com/total-number-of-websites/ [https://perma.cc/XXV4-A8XP].

ToS;DR that involve a larger group of human annotators face difficulty keeping pace. Many ToS;DR-reviewed services have a "No Class Yet" designation assigned where the ToS;DR team "think[s] [it] need[s] more reviews on that specific service before [it] can fully assess it." [156] Additionally, even for a number of mainstream services in widespread use like Facebook and Amazon, "No Class Yet" designations can still be found when ToS;DR feels that they have insufficient time and data to make an adequate comparison.[157] For ToS;DR, the process of scoring is time-consuming as it requires contributors to post a new thread or debate posts initiated by other users.[158] Dependence on participant input also means that the organization is unable to enforce any timelines. The dearth of contributor activity on the ToS;DR Google group suggests slow progress in scoring new services and also raises scalability concerns.[159] A system that relies upon such a time-intensive review process and significant user involvement is likely unsustainable.

Past attempts at privacy indicators suggest that technical limitations may also threaten an indicator's sustainability. One example of this is Privacy Bird, a browser plug-in that notified a user of whether a website's privacy practices matched the user's privacy preferences.[160] Though a survey of initial users determined that the service was downloaded 30,000 times before August 2002,[161] it remains all but unused as of July 2016.[162] This is because the tool only functions with older Microsoft Internet Explorer versions[163] and on privacy policies that implement P3P standards[164]—which are rarely used at present, as the World Wide Web Consortium suspended

[156] *See* Roy, *supra* note 9.

[157] *See Classification*, ToS;DR, *supra* note 31.

[158] *See id.*; *see also supra* note 55.

[159] As of July 7, 2016, eighty-five new threads had been opened in 2016, including discussions related to ToS;DR policy changes and spam. *See supra* note 55.

[160] *See* PRIVACY BIRD, http://www.privacybird.org/ [https://perma.cc/2NTL-SDK3].

[161] *See* Lorrie Faith Cranor et al., *User Interfaces for Privacy Agents*, 13 ACM TRANSACTIONS ON COMPUTER-HUM. INTERACTION (TOCHI) 135, 160 (2006).

[162] A Github account under the name Cristofer Mar published a Google Chrome extension for Privacy Bird downloaded only sixty-six times as of July 1, 2016. *See* Cristofer Mar (chrislmar), GITHUB, https://github.com/chrislmar [https://perma.cc/79E8-S27U] (last visited July 12, 2016).

[163] Specifically, Privacy Bird works on "Microsoft Internet Explorer 5.01, 5.5, and 6.0 web browsers on Microsoft Windows 98/2000/ME/NT/XP operating systems." *See* Lorrie Faith Cranor, Manjula Arjula & Praveen Guduru, *Use of a P3P User Agent by Early Adopters*, 2002 PROC. ACM WORKSHOP ON PRIVACY ELECTRONIC SOC'Y 1, 3 (2002) [hereinafter *Use of a P3P User Agent by Early Adopters*].

[164] *See id.* at 1–3.

development work in 2007.[165] Another example is the PlusPrivacy dashboard, and its technical limitation to certain browser extensions.[166]

In the case of PrivacyGrade.org, the utility of the initiative's 2012 and 2014 studies, which form the basis for its grades, is bound to expire. Moreover, cultural shifts in privacy policy perception by increasingly savvy internet users may ultimately nullify once-surprising elements on which the scheme's grading depends. For instance, a new study may reveal that internet user knowledge about and skepticism towards privacy practices has risen in the wake of widely reported data breaches or scandals like that regarding Cambridge Analytica,[167] bringing consumer privacy expectations more in line with actual practices. To remain sustainable, a successful privacy indicator must insure against technical limitations and be able to adapt over time.

IV. LAW AND POLICY REQUIREMENTS FOR SUCCESSFUL DEPLOYMENT OF PRIVACY INDICATORS

After identifying the obstacles that privacy indicator systems experience, the research seeks to map the law and policy needs for more meaningful, accurate, and adoptable rating indicators. To overcome the obstacles, we propose the following framework for adoption by policy-makers and industry to successfully deploy trustworthy and meaningful privacy indicators. Indicators can adequately, accurately, and successfully synthesize online privacy content if: (1) lawmakers or regulators establish standardized evaluation criteria as to the privacy practices to be considered and how these should be weighted in scoring techniques; (2) in the analytical and interpretive approach, rating mechanisms deployed by industry convey to users actual and demonstrable data practices, or simply show what a privacy statement says regarding recognized criteria rather than make deductive conclusions, and tools align with legal principles of contract interpretation and legal defaults as to the meaning of silence in privacy policy language; (3) a standardized system of icons is developed through government and industry collaborations, along with guidelines as to where

[165] *Status: P3P Work Suspended*, PLATFORM FOR PRIVACY PREFERENCES (P3P) PROJECT, http://www.w3.org/P3P/ [https://perma.cc/PCB7-H9NC]; *see also* Fred Langa, *Should I Turn on Internet Explorer's 'Enable Strict P3P Validation' Option?*, ITPRO TODAY (May 12, 2016), https://www.itprotod ay.com/windows-server/should-i-turn-internet-explorers-enable-strict-p3p-validation-option [https://pe rma.cc/4P76-NZ26].

[166] *See infra* Appendix.

[167] *See, e.g.*, Matthew Rosenberg & Gabriel J.X. Dance, '*You Are the Product': Targeted by Cambridge Analytica on Facebook*, N.Y. TIMES (Apr. 8, 2018), https://www.nytimes.com/2018/04/08/us/facebook-users-data-harvested-cambridge-analytica.html [https://perma.cc/RXT3-W6SL].

these should be presented; and (4) privacy raters are impartial, honest, autonomous, and financially and operationally durable.

A. Legislative or Regulatory Establishment of Standardized Evaluation Criteria

Nutrition and energy labeling criteria are standardized and established by governmental bodies.[168] Lawmakers and/or regulators should establish similar criteria objectively sufficient for evaluating online privacy protectiveness or invasiveness.[169] For example, guidance from the FTC or the Federal Communications Commission (FCC) in the United States, or the European Data Protection Supervisor, could evaluate proposals and articulate the required criteria. These criteria should specify both what factors are to be considered—privacy practices and specific data points—and how each of these aspects is to be judged and weighted. These criteria should be standardized across device operating systems, web platforms, and mobile applications.

The Model Privacy Form adopted under the Gramm-Leach-Bliley Act serves as an example of a successful regulatory effort to establish and implement standardized criteria. The model form was created as a tool for financial service providers to rely on to satisfy disclosure obligations under the Gramm-Leach-Bliley Act. The form was adopted by regulatory agencies after careful analysis and testing of language options.[170] In fact, eight federal financial service regulatory agencies approved the language used in this standardized privacy disclosure statement.[171]

For privacy indicators, the establishment of standardized evaluation criteria would dramatically reduce subjectivity and bias of the rating agent

[168] *See* Nutrition Labeling and Education Act (NLEA) of 1990, Pub. L. No. 101-535, 104 Stat. 2353 (codified as amended at 21 U.S.C. § 343 (2018)); U.S. FOOD AND DRUG ADMIN., GUIDANCE FOR INDUSTRY: FOOD LABELING GUIDE (2013), https://www.fda.gov/Food/GuidanceRegulation/GuidanceDocumentsRegulatoryInformation/LabelingNutrition/ucm2006828.htm [https://perma.cc/425F-WCXC]; National Energy Conservation Policy Act (NECPA) of 1978, 42 U.S.C. §§ 8201–8287d; *EnergyGuide Labels,* F.T.C., https://www.ftc.gov/news-events/media-resources/tools-consumers/energyguide-labels [https://perma.cc/8JQG-ZMLS].

[169] Ian Douglas, Tech. Analysis Directorate, Office of the Privacy Comm'r of Canada, Address at FTC PrivacyCon 2018: A Window into Internet of Things Privacy: Privacy Ratings for Internet-Enabled Health and Medical Devices (Feb. 28, 2018), https://www.ftc.gov/system/files/documents/public_events/1223263/panel018_iot_medical.pdf [https://perma.cc/C563-R5BD] (an example of regulatory leadership on establishing privacy grading criteria, presenting an approach for government-established criteria for rating privacy in health and medical devices).

[170] *See generally* ALAN LEVY & MANOJ HASTAK, CONSUMER COMPREHENSION OF FINANCIAL PRIVACY NOTICES: A REPORT ON THE RESULTS OF QUANTITATIVE TESTING (2008), http://www.sec.gov/comments/s7-09-07/s70907-21-levy.pdf [https://perma.cc/EGQ9-ZQH3].

[171] *See* FED. TRADE COMM'N, FINAL MODEL PRIVACY FORM UNDER THE GRAMM-LEACH-BLILEY ACT 1 (2009), https://www.ftc.gov/sites/default/files/documents/rules/privacy-consumer-financial-information-financial-privacy-rule/model_form_rule_a_small_entity_compliance_guide.pdf [https://perma.cc/M4FU-CKKJ].

and would produce a reasonable standard for grading rubrics. The absence of quantifiable measures in privacy policies has been recognized as an impediment to the development of successful privacy grading systems;[172] standardization would work toward remedying this shortcoming. Governmental creation of criteria also allows for more-fluid ability to adapt the standards over time as technologies, norms, and attitudes may change.

Others may then produce different indicator schemes—whether grades, labels, certifications, or dashboards—but each based on uniform baseline criteria. Consumers can utilize different tools they prefer based on visual aspects or other considerations without concern for the reliability of basic evaluation measures. Tools can also be produced based on the uniform criteria to more specifically gauge and compare privacy protection within certain industries or based on particular contexts online.

B. Analytical and Interpretative Approach

In order for privacy rating indicators to work, rating mechanisms deployed by industry must either convey to users actual data practices detected through technical means[173] or show what a privacy policy says with respect to recognized criteria rather than an interpretation of meaning. The latter shifts interpretive issues[174] to the user of the online service and allows him or her to individually determine how to reconcile ambiguity, vagueness, and inconsistency. Privacy indicators cannot successfully convey what policies "mean" in all instances to all users because of subjective preferences, interpretive differences, and the inherent ambiguity of privacy policies. Thus, pointing the user to specific language will often reduce interpretive errors of privacy indicators. Even if users prefer to be shown an absolute grade or score, this does not diminish the conceptual flaws that will either mislead users or misrepresent company policies.

Rating indicators must also align with legal principles of contract interpretation and legal defaults of silence. The entire policy must be interpreted as a whole document and not in isolated segments. In addition, unless statutory requirements exist to the contrary, silence must be treated in privacy-related conclusions as *permitting* the online service to engage in a certain data practice.

When determining how to label privacy language as to subject matter, developers of privacy tools should also be mindful to reduce ambiguity in

[172] *See* Kelley et al., *supra* note 1, at 5 ("[P]rivacy policies typically do not include quantifiable measures, and the P3P specification includes no quantifiable fields. The Kleimann Group dealt with this lack of quantifiable information by moving to binary Yes/No statements, which they found to be readily understood by focus group participants.").

[173] *See, e.g.*, *Welcome to Ghostery*, GHOSTERY, *supra* note 94.

[174] *See* Part III.0.

questions presented to annotators. Privacy indicator systems need to be based on unambiguous, objective prompts because it is impossible to eliminate ambiguity already existing in policy language. However, in an effort to prize conciseness and user-friendliness, privacy indicators should consider detracting marks for vagueness or ambiguity in language or providing a separate vagueness/clarity score. It may also be valuable, when interpretive issues exist, to provide ranges of agreement as to language interpretation rather than a rating system producing a definitive conclusion on meaning, again, shifting inevitable interpretative issues to individual users and the market.

C. Development of Standardized Icons, Location Placement, and Technical Requirements

A standardized system of icons, along with guidelines as to where these should be located, should also be developed through government and industry collaborations to reduce the education and learning curve now requisite for users to gain value from hosts of different and inconsistent privacy indicator systems. GDPR Article 12(7) already calls for "standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing."[175] Uniformity in the shorthand visual depictions developed will bolster universality and recognition, translating into greater consumer familiarity and utility.

Similarly, format standardization and consistent location make the process of identifying and comparing important privacy information easier and less time-consuming.[176] An example of what such an approach might look like is provided by Juro, which uses layering to present its privacy policies in digestible bits (here, "Types of data we collect," "How we use your data," and "Third parties who process your data").[177] Bullet points are offered under each category as well as an option to expand on the topic. Government guidance would assist industry to achieve such standardization and consistent location.

D. Reliability, Autonomy, and Sustainability of Indicator Systems

The research shows that each successful privacy indicator system must be reliable, autonomous, and operationally sustainable. Users must trust the

[175] GDPR, *supra* note 21, art. 12(7), at 40.

[176] Cranor, *supra* note 9, at 288.

[177] *Privacy by Design: Building a Privacy Policy People Actually Want to Read*, JURO (May 2, 2018), https://blog.juro.com/2018/05/02/privacy-by-design-building-a-privacy-policy-people-actually-want-to-read/ [https://perma.cc/8AAZ-PTXB].

validity and objectivity of the rating indicator.[178] For this to happen, rating consistency is key. The rater must adhere to its own policies and systems. The rater must also faithfully apply and weight its scoring criteria and must do so uniformly from policy to policy. Privacy ratings must also not need the consent of online services; they must operate autonomously irrespective of a website's or app's acquiescence to the privacy evaluation. Lastly, privacy indicator efforts must be capable of enduring, both financially and operationally. In addition to financial stability, rating systems must be automated to reduce needed human effort and be capable of canvassing a vast internet to produce and update output in real time.

CONCLUSION

If successful privacy indicators can be developed, the system of notice and choice in the United States will be much improved. These tools will also provide substantial benefit for internet users in the European Union and other jurisdictions where data protection regulation is based on consumer disclosure. However, although many have tried, efforts toward privacy ratings thus far have not been widely adopted.

Indicators of online privacy could gain traction if they are built on standardized evaluation criteria, produce objective and demonstrable output, are intelligible and accessible to users, and are reliable and sustainable long-term. Successful systems for privacy indicators will not only make disclosures more meaningful for users and empower users with enhanced ability for choice and control; they may also ratchet up aggregate privacy protections as well as nudge data processors toward specificity and clarity in privacy notices.

[178] Even industry-devised indicator systems such as those created by Google and Microsoft might be subject to external review to ensure objectivity. *See infra* Appendix, at pp. 41–42.

APPENDIX:
ADDITIONAL EFFORTS TOWARD PRIVACY INDICATORS

Privacy Grades and Scores:

Enonymous

Enonymous was launched in June 1998 and ended in 2000.[179] Users were required to download a software tool called Enonymous Adviser[180] that would display a privacy rating ranging from one to four stars in a pop-up window.[181] Ratings were based on a team of raters' efforts.[182] Poorly-rated or unrated websites would trigger a warning signal to the user.[183] Additionally, Enonymous offered a tool that would automatically fill in internet forms with user data stored in its database to an extent that such disclosure comported with user-preselected privacy preferences.[184]

DuckDuckGo

As of January 2018, search engine DuckDuckGo's browser extension and mobile app are equipped with a privacy enhancing and grading functionality.[185] When a user visits a website, DuckDuckGo will block tracker networks, switch from non-encrypted to encrypted site versions where available, and display a privacy grade in the extension icon. The privacy grade "score[s] automatically based on the prevalence of hidden tracker networks, encryption availability, and website privacy practices."[186] The privacy policy scores displayed, where available, are provided by Terms of Service; Didn't Read (ToS;DR).

[179] *See* Annie I. Antón & Julia B. Earp, A Taxonomy for Web Site Privacy Requirements 10 (Dec. 18, 2001) (unpublished manuscript), https://www.cc.gatech.edu/~aianton/assets/ataxonomyforwebsiteprivacy.pdf [https://perma.cc/EG5Y-CSU6].

[180] *See* Greenman, *supra* note 149.

[181] *See Odd Privacy Ratings Exposed*, *supra* note 117.

[182] Joel R. Reidenberg & Lorrie Faith Cranor, *Can User Agents Accurately Represent Privacy Notices?*, PROC. 30TH RES. CONF. ON COMM., INFO. & INTERNET POL'Y, at 12 n.27 (Aug. 30, 2002), https://ssrn.com/abstract=328860.

[183] *Id.*

[184] It is unclear whether users could choose to only allow the auto-fill function on websites rated above a certain number of stars. *See id.*

[185] *See* Gabriel Weinberg, *Protecting Your Personal Data Has Never Been This Easy*, DUCKDUCKGO (Jan. 23, 2018), https://spreadprivacy.com/privacy-simplified/ [https://perma.cc/W8GA-8WFL].

[186] *Id.*

Privacy Labels:

Privacy Bird

Privacy Bird is a software tool created to inform users how websites use their data,[187] originally created by AT&T and currently retained by the Carnegie Mellon University Usable Privacy and Security Laboratory (CUPS Lab).[188] Available online for free, Privacy Bird is a web browser add-on that automatically reads the privacy policies of websites a user visits.[189] It was made available through the now obsolete Platform for Privacy Preferences Project (P3P).[190] Based on preselected privacy preferences,[191] Privacy Bird notifies the user whether a website's privacy practices are above or below the level expected by the user.[192] If the privacy policy meets the user's preferences, Privacy Bird will display a green singing bird icon.[193] An exclamation mark appears next to the green bird when the website contains embedded content from other websites that do not have P3P privacy policies or have privacy features that do not meet the user's preferences.[194] If the policy does not match the user's preferences, a red bird icon displays, and when the website does not contain a P3P encoded privacy policy or when Privacy Bird fails to read the policy for some reason, a yellow bird icon appears.[195] Finally, when Privacy Bird is turned off, a

[187] PRIVACY BIRD, *supra* note 160.

[188] *Information for the Press*, PRIVACY BIRD, http://www.privacybird.org/press.html [https://perma.cc/4L59-7LD9].

[189] PRIVACY BIRD, *supra* note 160.

[190] *See supra* note 108. Developed by the World Wide Web consortium (W3C), P3P protocol allowed websites to declare their intended use of data collected from their users. Officially launched in 2002, results were mixed at best. Internet Explorer and Edge were some of the few browsers to adopt it, and by 2016 Microsoft announced that it would no longer support it on its Windows 10 system. *See P3P Is No Longer Supported*, MICROSOFT (Dec. 14, 2016), https://docs.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/mt146424(v=vs.85) [https://perma.cc/8LLU-KC4X]. According to Privacy Bird's website, earlier versions of Microsoft systems still support the tool. *See* PRIVACY BIRD, *supra* note 160.

[191] The Privacy Preference Settings menu first allows users to generally select a level of privacy between low, medium or high. Next, users may opt to receive warnings from the add-on when health or medical information, financial or purchase information, and non-personally identifiable information such as demographics, interests, or browsing history is used for analysis, marketing, or website customization and when the information is shared with third parties. Finally, for personally identifiable information, users can ask Privacy Bird to display when websites may contact the user for marketing purposes via telephone, email, or mail; when the websites do not allow a user to remove themselves from the mailing list, whether the website uses personally identifiable information to determine user habits, interests, characteristics, or shares the information with other companies; and when the website does not allow users to find out which information is collected. *Privacy Preferences*, PRIVACY BIRD, *supra* note 123.

[192] *Privacy Bird Tour*, *supra* note 123.

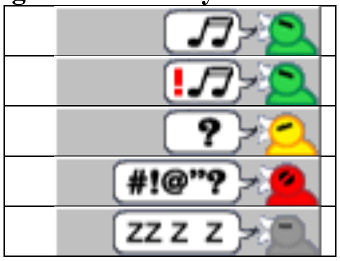
[193] *Id.*

[194] *Id.*

[195] *Id.*

grey bird appears.[196] Users can access the tool's menu, including the privacy settings selection form, by clicking on the bird icon.[197] The tool also contains a summary of the website's privacy policies.[198] The Privacy Bird icons are as follows:

Figure 1 – Privacy Bird Icons



European General Data Protection Regulation, Article 12(7)

The European Union's General Data Protection Regulation (GDPR) provides that a "data controller" must disclose certain information about its data practices to data subjects.[199] GDPR Article 12(1) requires that a data controller take "appropriate measures" to provide this information in a "concise, transparent, intelligible and easily accessible form."[200] Particularly relevant here, Article 12(7) provides that the information "may be provided in combination with standardized icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing."[201] This provision is intended to promote fair and transparent data processing.[202] Article 12(8) empowers the Commission to "adopt delegated acts[203] . . . [to determine] the information to be presented by the icons and the procedures for providing standardized icons."[204] Furthermore, Article 70(1)(r) charges the newly established European Data Protection Board with providing the Commission with "an opinion on the icons referred to in Article 12(7)."[205]

[196] *Id.*

[197] *See Use of a P3P User Agent by Early Adopters*, *supra* note 163.

[198] *Id.*

[199] *See* GDPR, *supra* note 21, art. 13, at 40; *see also id.* art. 14, at 41.

[200] *See id.* art. 12(1), at 39.

[201] *See id.* art. 12(7), at 40.

[202] *Id.*

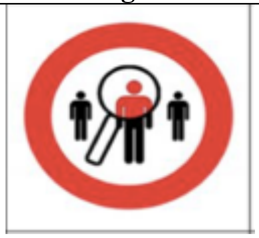
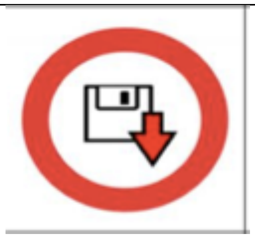
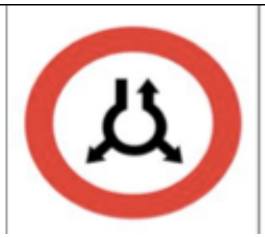
[203] Article 290 of the Treaty on the Functioning of the European Union (TFEU) allows the Parliament to delegate the "power to adopt non-legislative acts of general application to supplement or amend certain non-essential elements of a legislative act." *See* Consolidated Version of the Treaty on the Functioning of the European Union art. 290, May 9, 2008, 2008 O.J. (C 115) 47, 172.

[204] GDPR, *supra* note 21, art. 12(8), at 40.

[205] *Id.* art. 70, at 118.

The European Parliament’s draft, as initially reported out of committee, required six particular items to be disclosed using text and symbols.[206] Annex 1 of the Act, reproduced below in Figures 2 and 3, listed the required particulars and the symbols to be displayed.[207] However, the specific list of icons in the Annex is not part of the Act’s final text as the Parliament, the Commission, and the Council reached a compromise to simply empower the Commission to evaluate proposed icons.[208]

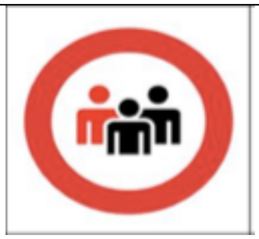
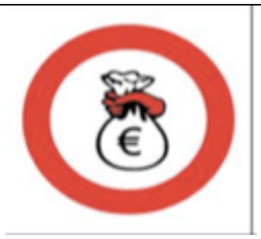
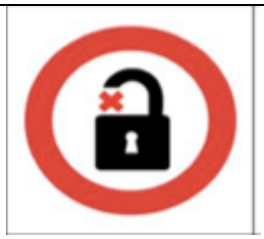
Figure 2 – Annex 1 Icons

	No personal data are collected beyond the minimum necessary for each specific purpose of the processing
	No personal data are retained beyond the minimum necessary for each specific purpose of the processing
	No personal data are processed for purposes other than the purposes for which they were collected

[206] Inofficial Consolidated Version After LIBE Committee Vote Provided by the Rapporteur, Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), art. 13a, at 43–44 (Oct. 22, 2013) https://www.janalbrecht.eu/wp-content/uploads/2018/05/DPR-Regulation-inofficial-consolidated-LIBE.pdf [https://perma.cc/VW5B-CPT3].

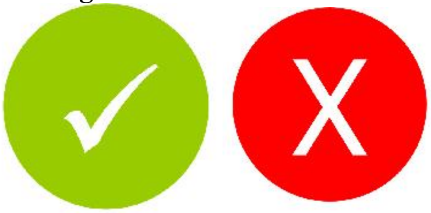
[207] *Id.* (Annex 1), at 115.

[208] *See generally* GDPR, *supra* note 21, art. 70, at 76. The trilogue meetings were held behind closed doors and the parties did not issue a final report. *See, e.g.*, Olivier Proust, *Unravelling the Mysteries of the GDPR Trilogues*, FIELDFISHER: PRIVACY, SEC. & INFO. LAW (July 16, 2015), http://privacylawblog. fieldfisher.com/2015/unravelling-the-mysteries-of-the-gdpr-trilogues/ [https://perma.cc/W6ZB-MVR M].

	No personal data are disseminated to commercial third parties
	No personal data are sold or rented out
	No personal data are retained in unencrypted form

Each of these icons would have been followed by one of the following, depending on the website data collection system.

Figure 3 – Annex 1 Icons



Know What's Inside and The App Association

Previously part of Moms With Apps (MWA), Know What's Inside was the product of a partnership between iOS developers and ACT | The App Association, which sought to promote quality apps and empower parents to choose the best ones for their children.[209] The service allowed parents to search for applications designed for children and filter results according to privacy preferences, target age, subject matter, and other criteria.[210] Every application had a description page, where an array of information is displayed in language intended for lay readers.[211] In relation to privacy, the description displayed limited amounts of text that inform parents about whether the app: (1) requires an internet connection; (2) collects personal data; (3) offers items for in-app purchase; (4) allows web browsing within the app; (5) shows information about related apps; (6) connects with social media; (7) contains in-app advertising; or (8) collects anonymous usage information.[212]

Today, Know What's Inside has morphed, and its concept has been integrated into, ACT | The App Association's platform. It still retains a page on the App Association's website, but the website's most recent content dates to 2013.[213] The App Association "represents more than 5,000 app companies and information technology firms . . . [advocating through its platform] for an environment that inspires and rewards innovation, while providing the necessary resources to help [its] members leverage their intellectual assets to raise capital, create jobs, and continue innovating."[214] The App Association also states that it seeks to promote data privacy through its "Privacy Resources" and "Privacy Dashboard" initiatives. Privacy Resources advocates for data privacy policy transparency and best practices for app developers through three sector-specific checklists: "Apps Directed to Children," "Health and Wellness Apps," and "Financial and Retail Apps."[215] Each page offers a checklist of best practices and links to regulation concerning each industry. The Privacy Dashboard provides a one-stop graphical interface for users to review app data usage.[216] An example of the Know What's Inside display is below.

[209] *See Discover Apps for Your Kids*, KNOW WHAT'S INSIDE, https://knowwhatsinside.com/discover [https://web.archive.org/web/20160429233918/https://knowwhatsinside.com/discover].

[210] *Id.*

[211] *About Know What's Inside*, KNOW WHAT'S INSIDE, https://knowwhatsinside.com/about [https://web.archive.org/web/20160429220606/https://knowwhatsinside.com/about].

[212] *See, e.g.*, *Peppy Pals Farm*, KNOW WHAT'S INSIDE, https://knowwhatsinside.com/peppy-pals/peppy-pals-empathy-adventures [https://web.archive.org/web/20160506112657/https://knowwhatsinside.com/peppy-pals/peppy-pals-empathy-adventures].

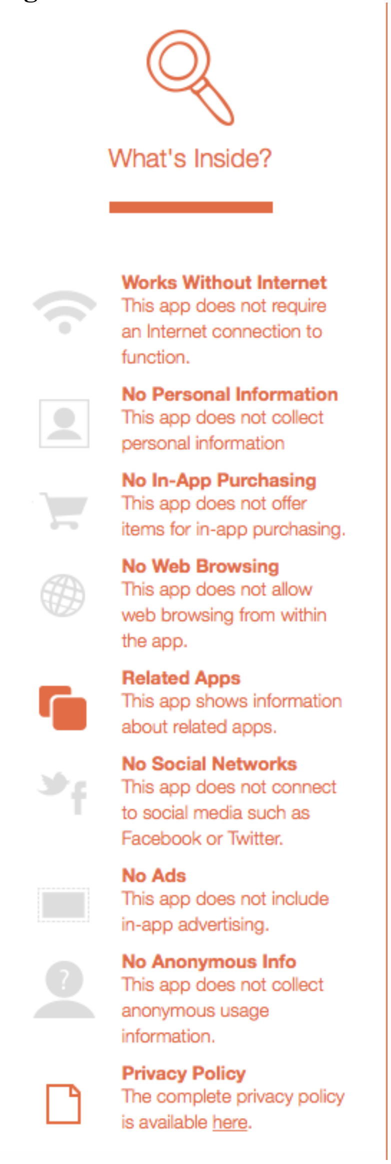
[213] *Know What's Inside COPPA and Privacy*, ACT | THE APP ASSOCIATION, http://actonline.org/knowwhatsinside/ [https://perma.cc/W86U-K9RW].

[214] *See* ACT | THE APP ASSOCIATION, https://actonline.org/ [https://perma.cc/8QV4-GK6K].

[215] *App Privacy and Transparency*, ACT: THE APP ASSOCIATION, https://actonline.org/privacy/ [https://perma.cc/A2RG-E5N9].

[216] *Privacy Dashboard*, ACT: THE APP ASSOCIATION, https://actonline.org/projects/privacy-dashboard/ [https://perma.cc/4RQB-CGZ2].

Figure 4 – Know What's Inside



What's Inside?

Works Without Internet
This app does not require an Internet connection to function.

No Personal Information
This app does not collect personal information

No In-App Purchasing
This app does not offer items for in-app purchasing.

No Web Browsing
This app does not allow web browsing from within the app.

Related Apps
This app shows information about related apps.

No Social Networks
This app does not connect to social media such as Facebook or Twitter.

No Ads
This app does not include in-app advertising.

No Anonymous Info
This app does not collect anonymous usage information.

Privacy Policy
The complete privacy policy is available here.

ESRB Ratings

The Entertainment Software Rating Board (ESRB) assigns badges that disclose whether entertainment software and applications, including websites and online gaming platforms,[217] comply with legal privacy requirements[218] and whether the software discloses user information.[219] Created in 1994 by the Entertainment Software Association, the ESRB is a "non-profit, self-regulatory body that assigns ratings for video games and apps so parents can make informed choices."[220] The ESRB badges and text messages signal age-appropriateness, content that may raise interest or concern, and interactive elements.[221] The last category tangentially addresses privacy concerns.[222]

The "Interactive Elements" disclosures include information as to whether the software: allows users to interact, possibly exposing them to "unfiltered/uncensored user-generated content . . . [and] sharing via social media"; shares a consumer's location with other users; and provides "unrestricted access to the internet."[223] For software sold at a retail store, the review process requires the software publisher to file a disclosure form and copies of relevant content prior to releasing the product, after which ESRB raters personally review the content and determine the ratings.[224] However, for software "available solely via download or accessible only online," the publisher must only submit a simplified disclosure form and the ratings are automatically assigned based on the publisher's disclosure.[225] To prevent abuses, the ESRB relies on "developers, the mobile community at large and storefronts that display ESRB ratings to identify rating issues whenever possible."[226] In an environment where gaming technology increasingly collects user data, such types of certification may become much more complex.[227]

Disconnect.me

Disconnect was founded in 2011 with online privacy at its core.[228] The company proposed a set of privacy icons that informed consumers of

[217] *See About ESRB*, ENTM'T SOFTWARE RATING BD., http://www.esrb.org/about/ [https://perma.cc/KMW6-38RA].

[218] *See ESRB Privacy Certified*, ENTM'T SOFTWARE RATING BD., *supra* note 104.

[219] *See ESRB Ratings Guide*, ENTM'T SOFTWARE RATING BD., http://www.esrb.org/ratings/ratings_guide.aspx [https://perma.cc/6GEG-BR8H].

[220] *About ESRB*, ENTM'T SOFTWARE RATING BD., *supra* note 217.

[221] *Id.*

[222] *See ESRB Ratings Guide*, ENTM'T SOFTWARE RATING BD., *supra* note 219.

[223] *See id.*

[224] *ESRB Ratings Process*, ENTM'T SOFTWARE RATING BD., http://www.esrb.org/ratings/ratings_process.aspx [https://perma.cc/ML4J-G2JZ].

[225] *Id.*

[226] *Id.*

[227] *See generally* N. Cameron Russell, Joel R. Reidenberg & Sumyung Moon, *Privacy in Gaming*, 29 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 61 (2018).

[228] *Who We Are*, DISCONNECT, https://disconnect.me/about [https://perma.cc/3G8S-A44R].

website data practices via a browser extension.[229] Its creators stated that the privacy icon system evolved from Mozilla's privacy icon project[230] and that the icons are "powered by data from the TRUSTe Privacy Policy Database."[231] Citing updating and proper functioning concerns, the browser extension has been delisted, but the company is looking into producing an updated version or a similar product in the future.[232] Disconnect continues to offer data and identity protection products and services.[233]

The Privacy Icon plug-in displayed icons in the user's browser to visually convey aspects of a website's privacy practices.[234] For example, the plug-in would display a green icon if the website is TRUSTe certified and a gray one if not.[235] The plug-in displayed icons representing the following: expected use (*i.e.*, whether the website's privacy policy discloses that the data it collects is used in ways other than a user would reasonably expect given the site's service), expected collection (*i.e.*, whether the website's privacy policy discloses whether it allows other companies such as ad providers and analytics firms to track users on the site), precise location data collection, user location tracking, data retention, compliance with users' do-not-track options, children's privacy, SSL support, whether a site is susceptible to certain malware viruses, and whether a site is TRUSTe Certified.[236]

[229] *Privacy Policies Are Too Complicated: We've Simplified Them*, DISCONNECT, https://web.archive.org/web/20160409094839/https://disconnect.me/icons [https://perma.cc/452C-TPVV] [hereinafter *Privacy Policies Are Too Complicated*].

[230] *See id.*

[231] *Id.*

[232] This paper's authors ascertained this through correspondence with the company on July 25, 2018.

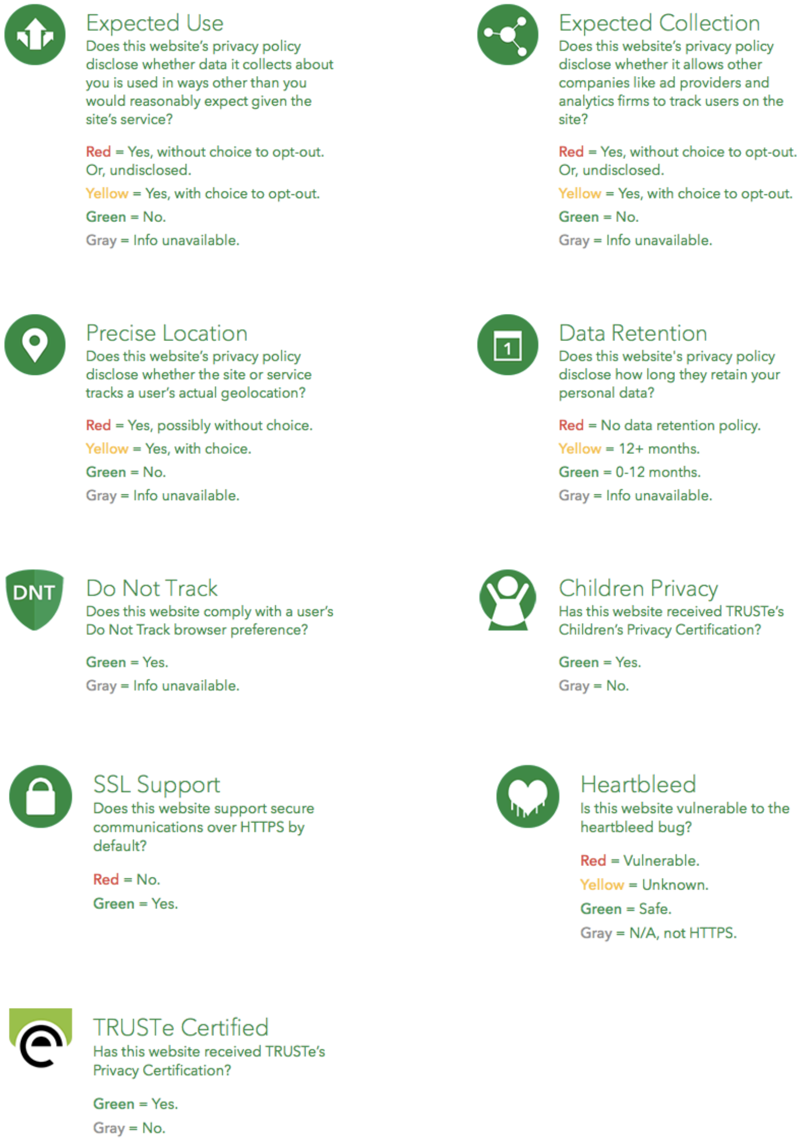
[233] DISCONNECT, https://disconnect.me/ [https://perma.cc/BM9R-27X9].

[234] *See Privacy Policies Are Too Complicated*, *supra* note 229.

[235] *Id.*

[236] *Id.*

Figure 5 – Disconnect.me Privacy Icons



Expected Use
Does this website's privacy policy disclose whether data it collects about you is used in ways other than you would reasonably expect given the site's service?

Red = Yes, without choice to opt-out. Or, undisclosed.
Yellow = Yes, with choice to opt-out.
Green = No.
Gray = Info unavailable.

Expected Collection
Does this website's privacy policy disclose whether it allows other companies like ad providers and analytics firms to track users on the site?

Red = Yes, without choice to opt-out. Or, undisclosed.
Yellow = Yes, with choice to opt-out.
Green = No.
Gray = Info unavailable.

Precise Location
Does this website's privacy policy disclose whether the site or service tracks a user's actual geolocation?

Red = Yes, possibly without choice.
Yellow = Yes, with choice.
Green = No.
Gray = Info unavailable.

Data Retention
Does this website's privacy policy disclose how long they retain your personal data?

Red = No data retention policy.
Yellow = 12+ months.
Green = 0-12 months.
Gray = Info unavailable.

Do Not Track
Does this website comply with a user's Do Not Track browser preference?

Green = Yes.
Gray = Info unavailable.

Children Privacy
Has this website received TRUSTe's Children's Privacy Certification?

Green = Yes.
Gray = No.

SSL Support
Does this website support secure communications over HTTPS by default?

Red = No.
Green = Yes.

Heartbleed
Is this website vulnerable to the heartbleed bug?

Red = Vulnerable.
Yellow = Unknown.
Green = Safe.
Gray = N/A, not HTTPS.

TRUSTe Certified
Has this website received TRUSTe's Privacy Certification?

Green = Yes.
Gray = No.

Privacy Certification Regimes and Seals:

Better Business Bureau Seal

The Better Business Bureau (BBB) generally seeks to promote transparency, honesty, and integrity in business practice and to foster consumer confidence by certifying companies that adhere to their guidelines.[237] BBB certifications are voluntary, and businesses must pay to obtain a BBB certification.[238] Section 7 of the BBB Accreditation Standards, "Safeguard Privacy," outlines the privacy-related criteria for obtaining a BBB certification; a website conducting electronic commerce must agree to disclose the following on their site: "what information they collect; with whom it is shared; how it can be corrected; how it is secured; how policy changes will be communicated; and how to address concerns over misuse of personal data."[239] Businesses seeking certification must ensure that they secure sensitive user data and must engage in "efforts to comply with industry standards for the protection and proper disposal of sensitive data."[240] Businesses must also "agree to respect customer preferences regarding contact by telephone, fax and email."[241]

ESRB Privacy Certified

In addition to its rating system, the ESRB certifies privacy compliance.[242] The ESRB started the Privacy Certified program in 1999 to "help interactive entertainment companies conduct business responsibly while assuring consumers, especially parents, that their personal data is collected and managed appropriately."[243] The three seals below certify compliance with domestic and international privacy laws such as the Children's Online Privacy Protection Act (COPPA) and the EU-U.S. Privacy Shield Framework:[244]

[237] *See BBB Accreditation Standards*, BETTER BUS. BUREAU, *supra* note 41.

[238] *See Apply for Accreditation Now*, BETTER BUS. BUREAU, *supra* note 110.

[239] *See BBB Accreditation Standards*, BETTER BUS. BUREAU, *supra* note 41.

[240] *Id.*

[241] *Id.*

[242] *See ESRB Privacy Certified*, ENTM'T SOFTWARE RATING BD., *supra* note 104.

[243] *ESRB Privacy Certified Member Services*, ENTM'T SOFTWARE RATING BD., http://www.esrb.org/privacy/member_services.aspx [https://perma.cc/E2TH-RESW]; *see also ESRB Privacy Certified Introduces New Services for Mobile Apps*, MARKETWIRED, *supra* note 102.

[244] *Frequently Asked Questions*, ENTM'T SOFTWARE RATING BD., http://www.esrb.org/privacy/faq.aspx#1 [https://perma.cc/N6QD-8JZD].

Figure 6 - ESRB Privacy Certified Seals

	The "ESRB Privacy Certified" seal signifies that a general audience website complies with applicable privacy laws and best practices related to the online collection and use of personal information.
	The "ESRB Privacy Certified for Kids" seal signifies that a child-directed website or app complies with applicable laws and requirements such as COPPA.
	The "ESRB Privacy Certified for Mobile" seal signifies that a mobile app complies with mobile privacy standards and best practices.

Additionally, Privacy Certified has personnel—including privacy attorneys—who offer privacy and data collection practices audits, privacy policy drafting, consulting, and dispute resolution services.[245] The ESRB website states that over 2,000 sites participate in their certification program.[246] To verify that a member site is in compliance with the ESRB standards, the site posts a "Click to Confirm" seal.[247]

Privacy Dashboards:

Google Dashboard

Launched in 2009, Google's Dashboard seeks to give users more control over their Google accounts by allowing them to review their Google-related activity, manage their privacy settings, save their data, view the company's privacy policies, and manage their Google services.[248] The Account review section permits consumers to review third-party apps with account access and displays what type of access they have along with a brief explanation.

[245] *See Monitoring & Consulting*, ENTM'T SOFTWARE RATING BD., *supra* note 48.

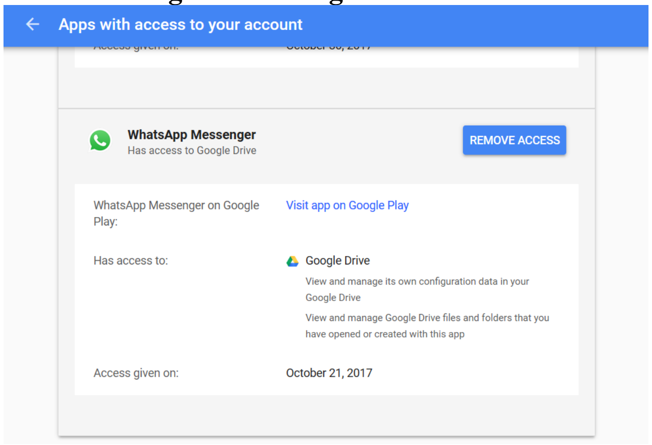
[246] *See ESRB Privacy Certified Member Services*, ENTM'T SOFTWARE RATING BD., *supra* note 243.

[247] *See id.*

[248] *Get a Summary of Data in Your Google Account*, GOOGLE, https://support.google.com/accounts/answer/162744?hl=en [https://perma.cc/X5WN-K6S2].

While the dashboard's utility is limited to Google and Google-connected third-party accounts, the ubiquity of Google services makes it relevant to most internet users.

Figure 7 – Google Dashboard



WhatsApp Messenger
Has access to Google Drive

WhatsApp Messenger on Google Play: Visit app on Google Play

Has access to: Google Drive
View and manage its own configuration data in your Google Drive
View and manage Google Drive files and folders that you have opened or created with this app

Access given on: October 21, 2017

Microsoft Privacy Dashboard

Similar to Google's Dashboard, Microsoft released its own Privacy Dashboard in early 2017.[249] It allows account holders to manage their privacy settings, and review and erase personal data Microsoft has saved with their account. The dashboard enables users to manage their browsing data, search history, location data, Cortana's Notebook, ad preferences, and apps and services allowed to access their data.[250]

PlusPrivacy

PlusPrivacy offers users a one-stop privacy dashboard. By using it, consumers can control their social media privacy settings, set up email aliases, block ads, monetize their information, and block unwanted apps and browser extensions from tracking them all from one place.[251] PlusPrivacy can be downloaded as an application or a plug-in and its code is open source,

[249] *Microsoft's New Privacy Dashboard and Set-up Experience Empowers Windows 10 Users*, MICROSOFT NEWS (Oct. 1, 2017), https://news.microsoft.com/europe/2017/01/10/privacy/ [https://perma.cc/T6WG-JXME].

[250] *Stay in Control of Your Privacy*, MICROSOFT, https://account.microsoft.com/account/privacy?refd=privacy.microsoft.com&ru=https%3A%2F%2Faccount.microsoft.com%2Fprivacy%3Frefd%3Dprivacy.microsoft.com&destrt=privacy-dashboard [https://perma.cc/E7XL-WRHW].

[251] *See* PLUSPRIVACY, *supra* note 97.

made available through GitHub.[252] Login-necessitating features, like creating email aliases, require setting a PlusPrivacy account.

In its browser extension version for Firefox and Chrome, PlusPrivacy assigns a privacy grade to other installed add-ons based on the permissions granted to it.[253] Privacy-centric add-ons like PlusPrivacy are given a "Privacy-oriented" label. The plug-in also lists permissions granted to Google, Facebook, Linkedin, Twitter, and Dropbox connected apps, but does not employ the same grading scheme as for extensions.[254] In its app form, PlusPrivacy provides a privacy level calculator which uses color icons and a "Privacy Pollution" number grade, where one is best and ten is worst, to rank a device's installed apps.[255] The apps are listed from least private (red) atop, to most private (green), below.[256] Icons vary in their shade of red, orange, yellow, and green according to their ranking.[257] Apps with the highest level of privacy receive a green shield icon. Selecting a graded app enables a user to uninstall the app or to view the permissions received.[258] These permissions are color-ranked as well according to PlusPrivacy's assessment of their intrusiveness.[259]

[252] *See OPERANDOH2020/PlusPrivacy*, GITHUB, *supra* note 98.

[253] *See infra* Figure 8(b).

[254] David Murphy, *Lock Down Your Social Media Data with the PlusPrivacy Chrome Extension*, LIFEHACKER (Mar. 21, 2018), https://lifehacker.com/lock-down-your-social-media-data-with-the-plusprivacy-c-1823961552 [https://perma.cc/5TPW-S5EG].

[255] *See infra* Figure 8(a).

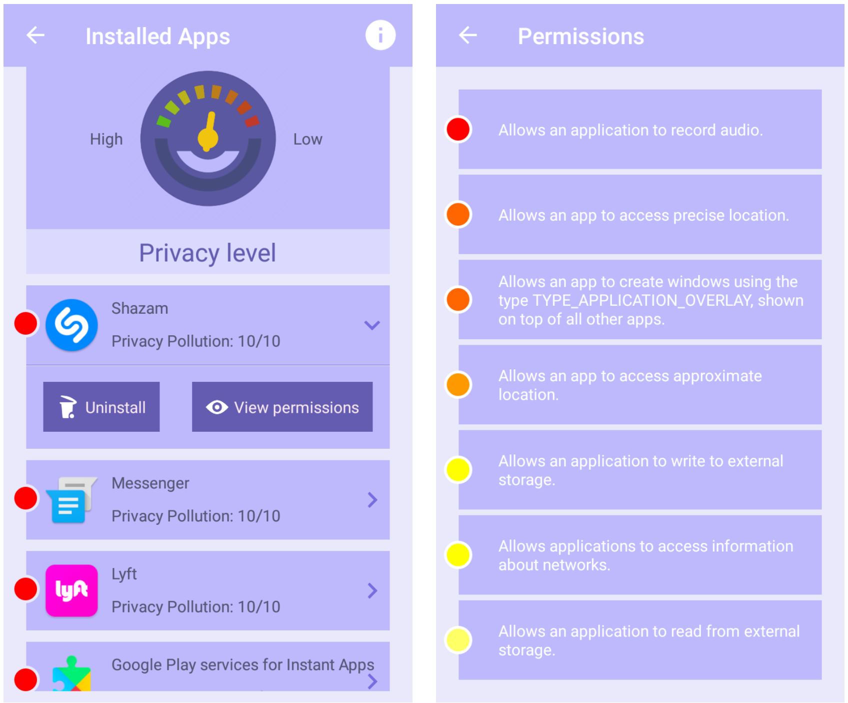
[256] *Id.*

[257] *Id.*

[258] *Id.*

[259] *Id.*

Figure 8(a) – PlusPrivacy Privacy level



Privacy level

Shazam
Privacy Pollution: 10/10

Messenger
Privacy Pollution: 10/10

Lyft
Privacy Pollution: 10/10

Google Play services for Instant Apps

● Allows an application to record audio.

● Allows an app to access precise location.

● Allows an app to create windows using the type TYPE_APPLICATION_OVERLAY, shown on top of all other apps.

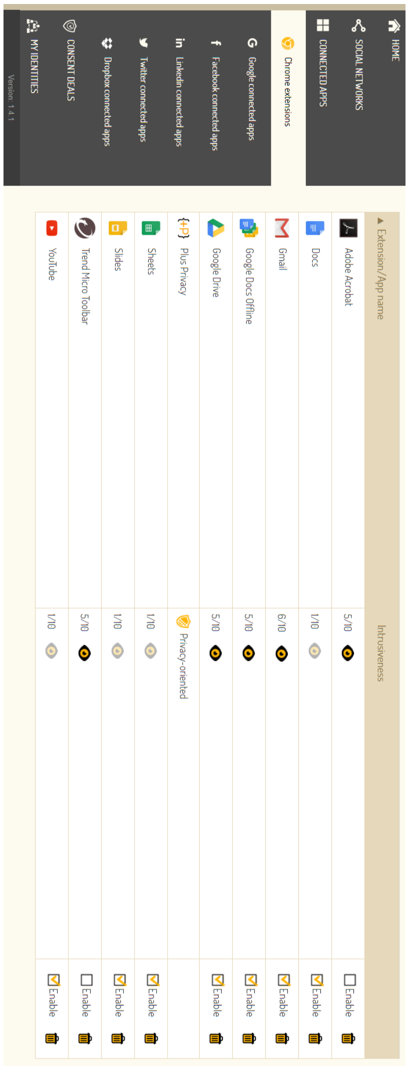
● Allows an app to access approximate location.

● Allows an application to write to external storage.

● Allows applications to access information about networks.

● Allows an application to read from external storage.

Figure 8(b) – PlusPrivacy Extension Grades



HOME
SOCIAL NETWORKS
CONNECTED APPS
Chrome extensions
Google connected apps
Facebook connected apps
LinkedIn connected apps
Twitter connected apps
Dropbox connected apps
CONSENT DEALS
MY IDENTITIES
Version: 1.4.1

▲ Extension/App name	Intrusiveness	
Adobe Acrobat	5/10	☐ Enable
Docs	1/10	☑ Enable
Gmail	6/10	☑ Enable
Google Docs Offline	5/10	☑ Enable
Google Drive	5/10	☑ Enable
Plus Privacy	Privacy-oriented	
Sheets	1/10	☑ Enable
Slides	1/10	☑ Enable
Trend Micro Toolbar	5/10	☐ Enable
YouTube	1/10	☑ Enable

PlusPrivacy is part of the OPERANDO project, a European Commission-funded initiative to "specify, implement, field-test, validate and exploit an innovative privacy enforcement platform that will enable the Privacy as a Service (PaS) business paradigm and the market for online privacy services."[260]

[260] *Objectives*, OPERANDO CONSORTIUM, https://www.operando.eu/servizi/Menu/dinamica.aspx?idSezione=17370&idArea=17829&idCat=17829&ID=17829&TipoElemento=area [https://perma.cc/9CEV-4ENE].