| Input Document | Identifiedby | Reviewedby / Link to | Status |
| --- | --- | --- | --- |
| [ICANN Procedure For Handling WHOIS Conflicts with Privacy Law](https://www.icann.org/resources/pages/whois-privacy-conflicts-procedure-2008-01-17-en) (2008)and [GNSO Policy underlying current procedure](http://gnso.icann.org/en/issues/whois-privacy/council-rpt-18jan06.htm) | Issue Report | [Metalitz](http://mm.icann.org/pipermail/gnso-rds-pdp-privacy/attachments/20160411/5082a7a5/Whoiosconflictschronandsummary7581581-0001.docx) | S |
| Review of the ICANN Procedure for Handling WHOIS Conflicts with Privacy Law (2014) | Issue Report | [Metalitz](http://mm.icann.org/pipermail/gnso-rds-pdp-privacy/attachments/20160411/5082a7a5/Whoiosconflictschronandsummary7581581-0001.docx) | S |
| 2013 RAA's [Data Retention Specification Waiver](https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#data-retention) and [Discussion Document](https://www.icann.org/en/system/files/files/draft-data-retention-spec-elements-21mar14-en.pdf) (2014) | Issue Report | Metalitz | A |
| [WHOIS Studies (2012-2014)](https://community.icann.org/pages/viewpage.action?pageId=56986688) , especially* [WHOIS Privacy/Proxy Abuse Study](http://www.icann.org/en/announcements/announcement-2-18may10-en.htm)
* [WHOIS Privacy/Proxy Relay and Reveal Survey](http://gnso.icann.org/issues/whois/whois-pp-relay-reveal-feasibility-survey-28mar11-en.pdf)
 | Charter |  |  |
| [SAC055, WHOIS: Blind Men and an Elephant](https://www.icann.org/en/system/files/files/sac-055-en.pdf) (September 2012) | Issue Report | [Folly](http://mm.icann.org/pipermail/gnso-rds-pdp-privacy/attachments/20160411/a8b721f3/SAC055_summary_Farell-0001.docx) | S |
| [Privacy & Proxy Services Accreditation PDP Final Report](http://gnso.icann.org/en/issues/raa/ppsai-final-07dec15-en.pdf) (2015) | Charter | [Metalitz](http://mm.icann.org/pipermail/gnso-rds-pdp-privacy/attachments/20160413/25b7f62b/PPSAIfinalreportsummaryforRDS-privacy7590780-0001.docx) | S |
| [Thick WHOIS PDP Final Report](http://gnso.icann.org/en/issues/whois/thick-final-21oct13-en.pdf) (2011-2013) and [IRT Legal Review](https://community.icann.org/download/attachments/52889541/ICANN%20Memorandum%20to%20the%20IRT%20-%20Thin%20to%20Thick%20WHOIS%20Transition_Final_2015-06-08.pdf) | Metalitz | [Metalitz](http://mm.icann.org/pipermail/gnso-rds-pdp-privacy/attachments/20160411/5082a7a5/SummaryofthickWhoisWGfinalreport--privacy7581437-0001.docx)[Metalitz](http://mm.icann.org/pipermail/gnso-rds-pdp-privacy/attachments/20160411/5082a7a5/summaryrethickWhoisIRTlegalreview7581532-0001.docx) | SS |
| Article 29 WP statement on the data protection impact of the ICANN RAA (2013-2014)- <https://www.icann.org/en/system/files/correspondence/namazi-to-kohnstamm-25mar14-en.pdf>- <https://www.icann.org/en/system/files/correspondence/kohnstamm-to-jeffrey-08jan14-en.pdf>- [https://www.icann.org/en/system/files/correspondence/jeffrey-to-kohnstamm-20sep13-- en.pdf](https://www.icann.org/en/system/files/correspondence/jeffrey-to-kohnstamm-20sep13-en.pdf)<https://www.icann.org/en/system/files/correspondence/kohnstamm-to-crocker-chehade-06jun13-en.pdf> | Issue Report | Sheckler | A |
| Article 29 WP comments on the data protection impact of the revision of the ICANN RAA concerning accuracy and data retention of WHOIS (2012)- <https://www.icann.org/en/system/files/correspondence/kohnstamm-to-crocker-atallah-26sep12-en.pdf>- <https://www.icann.org/en/news/correspondence/chehade-to-kohnstamm-09oct12-en> | Issue Report | [Ali](http://mm.icann.org/pipermail/gnso-rds-pdp-privacy/2016-April/000067.html) (p5) | S |
| Article 29 WP on ICANN Procedure for Handling WHOIS Conflicts with Privacy Law (2007)- <http://gnso.icann.org/en/correspondence/cerf-to-schaar-24oct07.pdf>- <https://www.icann.org/en/system/files/files/cerf-to-schaar-15mar07-en.pdf>- <https://www.icann.org/en/correspondence/schaar-to-cerf-12mar07.pdf> | Issue Report | [Walsh](http://mm.icann.org/pipermail/gnso-rds-pdp-privacy/attachments/20160413/3f92d28a/RDSPDPDocReview-A29WP-0001.docx) | S |
| Article 29 WP on ICANN’s WHOIS Database Policy (2006)- <https://www.icann.org/en/system/files/files/schaar-to-cerf-22jun06-en.pdf>- <https://www.icann.org/en/correspondence/lawson-to-cerf-22jun06.pdf>- <https://www.icann.org/en/correspondence/parisse-to-icann-22jun06.pdf>- <https://www.icann.org/en/system/files/files/fingleton-to-cerf-20jun06-en.pdf> | Issue Report | [Folly](http://mm.icann.org/pipermail/gnso-rds-pdp-privacy/2016-April/000090.html) | S |
| Article 29 WP Opinion on the application of the data protection principles to WHOIS directories [Article 29 WP 76 Opinion 2/2003](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp76_en.pdf)  | Issue Report | [Walsh](http://mm.icann.org/pipermail/gnso-rds-pdp-privacy/attachments/20160413/3f92d28a/RDSPDPDocReview-A29WP-0001.docx) | S |
| Additional Article 29 WP documents that may be of interest to this PDP WG | - | - | - |
| * [Article 29 WP 5 Recommendation 2/97](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1997/wp5_en.pdf)
 | Perrin | Sheckler | A |
| * [Article 29 WP 33 Opinion 5/2000](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2000/wp33_en.pdf)
 | Perrin | Sheckler | A |
| * [Article 29 WP 41](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp41_en.pdf) [Opinion 4/2001](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp41_en.pdf)
 | Perrin | Sheckler | A |
| * [Article 29 WP 56 Working Document 5/2002](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2002/wp56_en.pdf)
 | Perrin | Sheckler | A |
| * [Article 29 WP 217 Opinion 6/2014](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf)
 | Kimpian | Perrin | A |
| * [Article 29 WP Opinion 1/2010](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf)
 | Perrin | Perrin | A |
| * [Article 29 WP 20 Opinion 3/1999](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1999/wp20_en.pdf)
 | Ali | [Ali](http://mm.icann.org/pipermail/gnso-rds-pdp-privacy/2016-April/000083.html) | S |
| Council of Europe Declaration | - | - | - |
| * [Declaration of Committee of Ministers on ICANN, human rights and the rule of law](https://wcd.coe.int/ViewDoc.jsp?Ref=Decl%2803.06.2015%292) (3 June 2015)
 | Kimpian | Sheckler | A |
| * [Council of Europe's Treaty 108 on Data Protection](http://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/108)
 | Kleiman | [Kleiman](http://mm.icann.org/pipermail/gnso-rds-pdp-privacy/attachments/20160410/74fe4bcd/CouncilofEuropesTreaty108onDataProtections-0001.doc) | S |
| EDPS Correspondence regarding Registration Data | - | - | - |
| * [Opinion of the European Data Protection Supervisor: Europe's role in shaping the future of Internet Governance](https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-06-23_Internet_Governance_EN.pdf) (23 June 2014)
 | Perrin | [Ferdeline](http://mm.icann.org/pipermail/gnso-rds-pdp-privacy/2016-April/000070.html) | S |
| * [ICANN's public consultation on 2013 RAA Data Retention Specification Data Elements and - Legitimate Purposes for Collection and Retention](https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2014/14-04-17_EDPS_letter_to_ICANN_EN.pdf) (17 April 2014)
 | Kimpian | [Ferdeline](http://mm.icann.org/pipermail/gnso-rds-pdp-privacy/2016-April/000069.html) | S |
| [European Commission Website: Obligations of Data Controllers](http://ec.europa.eu/justice/data-protection/data-collection/obligations/index_en.htm) | Kleiman | [Kleiman](http://mm.icann.org/pipermail/gnso-rds-pdp-privacy/attachments/20160410/74fe4bcd/SummaryofEUCommissionWebsite_ObligationsofDataControllers-0001.doc) | S |
| [European Commission News Announcement: EU-US Privacy Shield](http://ec.europa.eu/justice/newsroom/data-protection/news/160229_en.htm) | Kleiman | [Kleiman](http://mm.icann.org/pipermail/gnso-rds-pdp-privacy/attachments/20160410/74fe4bcd/SummaryEurCommnNewAnnouncement_EUandUSPrivacyShield-0001.doc) | S |
| [European Data Protection Directive, 1995](http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al14012) | Kleiman | [Kleiman](http://mm.icann.org/pipermail/gnso-rds-pdp-privacy/attachments/20160410/74fe4bcd/EuropeanDataProtectionDirective1995-0001.doc) | S |
| International Working Group on Data Protection in Telecommunications and Media Documents | - | - | - |
| * [Common Position relating to Reverse Directories](https://datenschutz-berlin.de/attachments/176/rever_en.pdf?1201099194) (Hong Kong, 15.04.1998)
 | Perrin | [Ali](http://mm.icann.org/pipermail/gnso-rds-pdp-privacy/2016-April/000067.html) (p4) | S |
| * [Common Position on Privacy and Data Protection aspects of the Registration of Domain Names on the Internet](https://datenschutz-berlin.de/attachments/222/dns_en.pdf?1200656953) (Crete, 4./5.05.2000)
 | Perrin | [Ali](http://mm.icann.org/pipermail/gnso-rds-pdp-privacy/2016-April/000067.html) (p3) | S |
| * [Common Position on Privacy and Data Protection aspects of the Publication of Personal Data contained in publicly available documents on the Internet](https://datenschutz-berlin.de/attachments/220/pd_en.pdf?1201099774) (Crete, 4./5.05.2000)
 | Perrin | [Ali](http://mm.icann.org/pipermail/gnso-rds-pdp-privacy/2016-April/000083.html)  | S |
| * [Common Position on Incorporation of telecommunications-specific principles in multilateral privacy agreements: Ten Commandments to protect Privacy in the Internet World](https://datenschutz-berlin.de/attachments/216/tc_en.pdf?1200658742) (Berlin, 13/14.09.2000)
 | Perrin | [Ali](http://mm.icann.org/pipermail/gnso-rds-pdp-privacy/2016-April/000067.html) (p2) | S |
| * [Common Position on data protection aspects in the Draft Convention on cyber-crime of the Council of Europe](https://datenschutz-berlin.de/attachments/218/cy_en.pdf?1200656876) (Berlin, 13/14.09.2000)
 | Perrin | [Ali](http://mm.icann.org/pipermail/gnso-rds-pdp-privacy/2016-April/000067.html) (p1) | S |
| [NORC Study of WHOIS Privacy/Proxy Prevalence](https://www.icann.org/en/system/files/newsletters/privacy-proxy-registration-services-study-14sep10-en.pdf) (2010) | Issue Report | [Coupet](http://mm.icann.org/pipermail/gnso-rds-pdp-privacy/attachments/20160412/4a17077a/privacy-proxy-registration-services-study-14sep10-en_PDP-0001.docx) | S |
| [EWG Recommendations for a Next-Generation RDS](https://www.icann.org/en/system/files/files/final-report-06jun14-en.pdf), especially* Section 6a, Data Protection Principles
* Section 6b, Principles for Data Access by Law Enforcement
* Section 7, Improving Registrant Privacy
* Annex H, Model for Relay and Reveal
 | Charter | [Samuels](http://mm.icann.org/pipermail/gnso-rds-pdp-privacy/2016-April/000073.html) | S |
| EWG Research: [Data Protection Considerations Applicable to Collection of gTLD Reg Data Memo](https://community.icann.org/download/attachments/43982771/Memo%20to%20EWG%20re%20gTLD%20Registration%20Data%20and%20International%20Data%20Privacy%20Considerations.docx) | Framework | [Coupet](http://mm.icann.org/pipermail/gnso-rds-pdp-privacy/attachments/20160412/4a17077a/MemotoEWGregTLDRegistrationDataandInternationalDataPrivacyConsiderations-Summary-0001.docx) | S |
| EWG Research: [WHOIS Privacy and Proxy Service Provider Practices Survey](https://community.icann.org/download/attachments/45744698/EWG%20PP%20PROVIDER%20QUESTIONNAIRE%20SUMMARY%2014%20March%202014.pdf) | Charter |  |  |
| [EWG Tutorial](http://london50.icann.org/en/schedule/mon-ewg-final-overview/presentation-ewg-final-overview-23jun14-en.pdf) Pages 28-30 and [EWG FAQs](https://community.icann.org/display/EWG/EWG%2BFAQs) 31-38 | Issue Report |  |  |
| Statements/Blogs by [Ajayi](http://www.circleid.com/posts/20141105_how_to_improve_whois_data_accuracy/) and [Perrin](https://www.icann.org/en/system/files/files/perrin-statement-24jun14-en.pdf) | Issue Report |  |  |
| [Process Framework](https://community.icann.org/display/gTLDRDS/Process%2BFramework) for a PDP on Next-Generation RDS, especially Page 9, Row 5 | Charter |  |  |
| [Human Rights Council - Report by the UN Special Rapporteur on the right to privacy](http://www.ohchr.org/Documents/Issues/Privacy/A-HRC-31-64.doc)  | Ferdeline |  |  |
| EU Court of Justice Judgements that may apply to gTLDs, including | - | - | - |
| * [Judgement on preliminary ruling under Article 267 TFEU from Audiencia Nacional (Spain)](http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=11654)
 | Ferdeline |  |  |
| * [Judgment of the Court (Grand Chamber) - Maximillian Schrems v Data Protection Commissioner](http://curia.europa.eu/juris/liste.jsf?pro=&lgrec=en&nat=or&oqp=&dates=&lg=&language=en&jur=C%2CT%2CF&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&num=C-362%252F14&td=%3BALL&pcs=Oor&avg=&page=1&mat=or&jge=&for=&cid=576711)
 | Kleiman | Kleiman | A |
| [Africa Union Convention on Cybersecurity and Personal Data Protection](http://pages.au.int/sites/default/files/en_AU%20Convention%20on%20CyberSecurity%20Pers%20Data%20Protec%20AUCyC%20adopted%20Malabo.pdf) | Mutung'u | [Mutung'u](http://mm.icann.org/pipermail/gnso-rds-pdp-privacy/attachments/20160413/85aed499/AUCCyPdp-0001.docx) | S |
| Relevant National Laws or Court Rulings that may apply to gTLDs, including* [US Supreme Court Case - McIntyre v. Ohio Elections Commission, 514 U.S. 334 (1995](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwj4lJqo9e3LAhWEzoMKHTwqCioQFggdMAA&url=https%3A%2F%2Fwww.law.cornell.edu%2Fsupct%2Fhtml%2F93-986.ZO.html&usg=AFQjCNHPC2JbcoTHCuLOt78Rdf-abDI8vg))
* [The Constitution of the State of California (USA): Article 1, Section 1](http://www.leginfo.ca.gov/.const/.article_1)
* [Massachusetts Right of Privacy, MGL c.214, s.1B](https://malegislature.gov/Laws/GeneralLaws/PartIII/TitleI/Chapter214/Section1B)
* [US Judicial Redress Act of 2015](https://www.govtrack.us/congress/bills/114/hr1428)
* [Ghana Protection Act, 2012](http://media.mofo.com/files/PrivacyLibrary/3981/GHANAbill.pdf)
* [South Africa’s Act No. 4 of 2013: Protection of Personal Information Act](http://www.justice.gov.za/legislation/acts/2013-004.pdf)
 | KleimanKleimanKleimanKleimanMutung'uMutung'u | Kleiman [Kleiman](http://mm.icann.org/pipermail/gnso-rds-pdp-privacy/attachments/20160414/38414cc4/SummaryofConstitutionofCaliforniaArticle1Section1-0001.doc)[Kleiman](http://mm.icann.org/pipermail/gnso-rds-pdp-privacy/attachments/20160414/38414cc4/SummaryofMassachusettsPrivacyLaw-0001.doc)[Kleiman](http://mm.icann.org/pipermail/gnso-rds-pdp-privacy/attachments/20160414/38414cc4/SummaryofUSJudicialRedressAct2_2016-0001.doc)[Mutung'u](http://mm.icann.org/pipermail/gnso-rds-pdp-privacy/attachments/20160413/85aed499/Ghana-0001.docx)[Mutung'u](http://mm.icann.org/pipermail/gnso-rds-pdp-privacy/attachments/20160413/85aed499/SouthAfrica-0001.docx) | ASSSSS |
| [Governance of Privacy: Policy Instruments in Global Perspective](https://mitpress.mit.edu/books/governance-privacy)  (MIT Press 2006) | Perrin |  |  |
| Book: [Global Tables of Data Privacy Laws and Bills (Greenleaf, 4rd Edition, January 2015)](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2603502) | Perrin | [Kleiman](http://mm.icann.org/pipermail/gnso-rds-pdp-privacy/attachments/20160414/38414cc4/SummaryofGlobalTablesofDataPrivacyLawsandBillsProfessorGreenleaf-0001.doc) | S |
| [Article: Global data privacy laws 2015: 109 countries, with European laws now a minority (Greenleaf)](http://ssrn.com/abstract%3D2603529) | Kleiman | [Kleiman](http://mm.icann.org/pipermail/gnso-rds-pdp-privacy/attachments/20160414/38414cc4/SummaryGlobaldataprivacylaws2015byProfessorGreenleaf-0001.doc) | S |
| [WorldLII Database of National Data Privacy Legislation](http://www.worldlii.org/int/other/NDPrivLegis) | Kleiman |  |  |

Note: Relevant input documents not already on the starter list may continue to be added by team members.
All additions will be appended to the end of the table unless they clearly fit within an existing category of documents already identified.

“Identified by” indicates who first identified the document as input – in several cases, the same document was suggested more than once.

“Reviewed by” indicates which member of this small team:

* already posted a summary of the document, focusing on portions relevant to Privacy (follow hyperlink for submitted summary), or
* has volunteered to summarize portions of the document relevant to Privacy.

“Status” indicates the summary has been (A)ssigned to the reviewer, (S)ubmitted to the email list, or determined by the team to be (C)omplete.

-[EWG member] Statements/Blogs by Perrin and Ajayi

-EWG Research: WHOIS Privacy and Proxy Service Provider Practices Survey
-EWG Tutorial Pages 28-30 and EWG FAQs 31-38
-Process Framework for a PDP on Next-Generation RDS, especially Page 9, Row 5
-Human Rights Council - Report by the UN Special Rapporteur on the right to privacy
-Judgement on preliminary ruling under Article 267 TFEU from Audiencia Nacional (Spain)
-WorldLII Database of National Data Privacy Legislation (do not need to review the database, just summarize its relevance to this PDP)

How to mitigate effects of loss of privacy due to the business model of the Internet, which is suveillance?

1. Transparency trap: Consumer empowerment is a myth,
* since the consumer is the product;
* multiple sources of data collection, proprietary algorythms
1. Individualistic market-based solutions are not the solution (‘opt-out clauses’) because Internet is consumer-facing with sociology of consumer reasoning: we’d rather trade of our privacy for shot-term (immediate) gains even if harm is possible in a distant future
* Need for a more benevolent ‘paternalistic’ and structural approach

Solutions:

1) 1st party engagement: no surveillance if you don’t go on the company’s website (// banks that are too big to fail, surveillance company would be too big)

1. Ban reselling = repurposing of data
2. Limit data retention to days or months, then potential for abuse and surveillance is dramatically reduced.

# Anonymity is the internet's next big battleground

Users are growing twitchy about how their data is being used, with major ramifications for advertisers, marketers and the entire internet industry

Online users are rebelling against those tracking and snooping them by adopting a variety of privacy tools. Photograph: Epoxydude/Corbis

[**Jon Card**](http://www.theguardian.com/profile/jon-card)

Monday 22 June 2015 07.00 EDTLast modified on Monday 22 June 201508.17 EDT

[**Save for later**](https://profile.theguardian.com/save-content?INTCMP=DOTCOM_ARTICLE_SFL&returnUrl=http%3A%2F%2Fwww.theguardian.com%2Fmedia-network%2F2015%2Fjun%2F22%2Fanonymity-internet-battleground-data-advertisers-marketers&shortUrl=/p/49zmm&platform=web:Chrome:wide)

The use of personal data is a thorny subject for the public and for the many companies that use it. By allowing companies to take their data, internet users are enabling the creation of a fast, free and relevant online experience. But more recently the scale of this data gathering and the way it is then traded, analysed and used has come under greater scrutiny.

Users seem less willing to go along with this “trade off” in a [post-Snowden age](http://www.theguardian.com/us-news/edward-snowden)and some are rebelling against those tracking and snooping on them. Searchers are increasingly adopting privacy tools and ad blocking plug-ins, private search engines such as [DuckDuckGo](http://www.theguardian.com/technology/2014/apr/04/duckduckgo-gabriel-weinberg-secure-searches) and anonymous browsers such as [Tor](http://www.theguardian.com/technology/2013/nov/05/tor-beginners-guide-nsa-browser) to prevent their data being taken.

David Benigson, CEO of media intelligence and information discovery platform[Signal](http://signal.uk.com/), is one industry figure who believes concerns over privacy are causing a big change in user behaviour. “As people have become more aware of the potential for their online activities to be used in ways they hadn’t necessarily intended, usage of encrypted browsers, ad-blockers and other anonymising devices has soared,” he says. “Historically, web giants have managed to convince consumers into giving up their privacy – the fact that every Google search is logged and recorded, for example, is now seen as par for the course. The fact that consumers willingly or unwilling give up vast amounts of private data and then this data is used in a whole spectrum of ways that the user is unaware of, feels like a pretty poor model.”

# Analysis Beware a future where health monitoring by wearables is the norm

As wearable devices are equipped with advanced health-tracking technology, how long before third parties use this information to gauge how well we are?

Read more

**Disparity between what users think and how they behave**

Studies suggest privacy is a growing concern. Research by [Global Web Index](http://www.globalwebindex.net/blog/vpn-infographic)found that 27% of adult online users had utilised a virtual private network ([VPN](https://en.wikipedia.org/wiki/Virtual_private_network)) to access the internet. Meanwhile, [The State of Privacy Report 2015](https://www.symantec.com/content/en/us/about/presskits/b-state-of-privacy-report-2015.pdf)(pdf), commissioned by anti-virus company Symantec, which interviewed more than 7,000 internet users across Europe, found that 57% of people are worried their data is not safe. Meanwhile, only 14% of internet users were happy for businesses to share their data with third parties.

But the report found a disparity between what users think and how they actually behave. Just one in four users read the terms and conditions before signing up to an online service and the authors felt that many users didn’t know how to protect their data. In conclusion, the report stated: “Despite much concern about the security and privacy of data, many are unsure what to do to better protect their data … the behaviour of many Europeans is not reflected by their actions towards data protection.”

### [media & tech network](https://adclick.g.doubleclick.net/aclk%253Fsa%253DL%2526ai%253DBasvHVs0nV92yLI7PBe6To-gPp5nBgAgAAAAQASDvlN8hOABY79iC4v0BYMmGgIDco8QQsgETd3d3LnRoZWd1YXJkaWFuLmNvbboBCWdmcF9pbWFnZcgBCdoBb2h0dHA6Ly93d3cudGhlZ3VhcmRpYW4uY29tL21lZGlhLW5ldHdvcmsvMjAxNS9qdW4vMjIvYW5vbnltaXR5LWludGVybmV0LWJhdHRsZWdyb3VuZC1kYXRhLWFkdmVydGlzZXJzLW1hcmtldGVyc6kCizxWm0mcuD7AAgLgAgDqAjIvNTk2NjYwNDcvdGhlZ3VhcmRpYW4uY29tL21lZGlhLW5ldHdvcmsvYXJ0aWNsZS9uZ_gC9NEekAPgA5gDjAaoAwHQBJBO4AQB0gUFEOeY9SWQBgGgBh_YBwDgBxs%2526num%253D0%2526cid%253DCAASEuRourlbFbnCT8eNqxFtsyqUSw%2526sig%253DAOD64_3LLauHW1d0ABDBcD-tH5-MgeQSpA%2526client%253Dca-pub-4830087483992392%2526adurl%253Dhttp%3A/register.theguardian.com/media/)

[](https://adclick.g.doubleclick.net/aclk%253Fsa%253DL%2526ai%253DBasvHVs0nV92yLI7PBe6To-gPp5nBgAgAAAAQASDvlN8hOABY79iC4v0BYMmGgIDco8QQsgETd3d3LnRoZWd1YXJkaWFuLmNvbboBCWdmcF9pbWFnZcgBCdoBb2h0dHA6Ly93d3cudGhlZ3VhcmRpYW4uY29tL21lZGlhLW5ldHdvcmsvMjAxNS9qdW4vMjIvYW5vbnltaXR5LWludGVybmV0LWJhdHRsZWdyb3VuZC1kYXRhLWFkdmVydGlzZXJzLW1hcmtldGVyc6kCizxWm0mcuD7AAgLgAgDqAjIvNTk2NjYwNDcvdGhlZ3VhcmRpYW4uY29tL21lZGlhLW5ldHdvcmsvYXJ0aWNsZS9uZ_gC9NEekAPgA5gDjAaoAwHQBJBO4AQB0gUFEOeY9SWQBgGgBh_YBwDgBxs%2526num%253D0%2526cid%253DCAASEuRourlbFbnCT8eNqxFtsyqUSw%2526sig%253DAOD64_3LLauHW1d0ABDBcD-tH5-MgeQSpA%2526client%253Dca-pub-4830087483992392%2526adurl%253Dhttp%3A/register.theguardian.com/media/)

#### **[Sign up to the Media & Tech network](https://adclick.g.doubleclick.net/aclk%253Fsa%253DL%2526ai%253DBasvHVs0nV92yLI7PBe6To-gPp5nBgAgAAAAQASDvlN8hOABY79iC4v0BYMmGgIDco8QQsgETd3d3LnRoZWd1YXJkaWFuLmNvbboBCWdmcF9pbWFnZcgBCdoBb2h0dHA6Ly93d3cudGhlZ3VhcmRpYW4uY29tL21lZGlhLW5ldHdvcmsvMjAxNS9qdW4vMjIvYW5vbnltaXR5LWludGVybmV0LWJhdHRsZWdyb3VuZC1kYXRhLWFkdmVydGlzZXJzLW1hcmtldGVyc6kCizxWm0mcuD7AAgLgAgDqAjIvNTk2NjYwNDcvdGhlZ3VhcmRpYW4uY29tL21lZGlhLW5ldHdvcmsvYXJ0aWNsZS9uZ_gC9NEekAPgA5gDjAaoAwHQBJBO4AQB0gUFEOeY9SWQBgGgBh_YBwDgBxs%2526num%253D0%2526cid%253DCAASEuRourlbFbnCT8eNqxFtsyqUSw%2526sig%253DAOD64_3LLauHW1d0ABDBcD-tH5-MgeQSpA%2526client%253Dca-pub-4830087483992392%2526adurl%253Dhttp%3A/register.theguardian.com/media/)**

[Sign up today and receive exclusive member newsletters, networking opportunities, member-only discounts and more.](https://adclick.g.doubleclick.net/aclk%253Fsa%253DL%2526ai%253DBasvHVs0nV92yLI7PBe6To-gPp5nBgAgAAAAQASDvlN8hOABY79iC4v0BYMmGgIDco8QQsgETd3d3LnRoZWd1YXJkaWFuLmNvbboBCWdmcF9pbWFnZcgBCdoBb2h0dHA6Ly93d3cudGhlZ3VhcmRpYW4uY29tL21lZGlhLW5ldHdvcmsvMjAxNS9qdW4vMjIvYW5vbnltaXR5LWludGVybmV0LWJhdHRsZWdyb3VuZC1kYXRhLWFkdmVydGlzZXJzLW1hcmtldGVyc6kCizxWm0mcuD7AAgLgAgDqAjIvNTk2NjYwNDcvdGhlZ3VhcmRpYW4uY29tL21lZGlhLW5ldHdvcmsvYXJ0aWNsZS9uZ_gC9NEekAPgA5gDjAaoAwHQBJBO4AQB0gUFEOeY9SWQBgGgBh_YBwDgBxs%2526num%253D0%2526cid%253DCAASEuRourlbFbnCT8eNqxFtsyqUSw%2526sig%253DAOD64_3LLauHW1d0ABDBcD-tH5-MgeQSpA%2526client%253Dca-pub-4830087483992392%2526adurl%253Dhttp%3A/register.theguardian.com/media/)

[**Click here**](https://adclick.g.doubleclick.net/aclk%253Fsa%253DL%2526ai%253DBasvHVs0nV92yLI7PBe6To-gPp5nBgAgAAAAQASDvlN8hOABY79iC4v0BYMmGgIDco8QQsgETd3d3LnRoZWd1YXJkaWFuLmNvbboBCWdmcF9pbWFnZcgBCdoBb2h0dHA6Ly93d3cudGhlZ3VhcmRpYW4uY29tL21lZGlhLW5ldHdvcmsvMjAxNS9qdW4vMjIvYW5vbnltaXR5LWludGVybmV0LWJhdHRsZWdyb3VuZC1kYXRhLWFkdmVydGlzZXJzLW1hcmtldGVyc6kCizxWm0mcuD7AAgLgAgDqAjIvNTk2NjYwNDcvdGhlZ3VhcmRpYW4uY29tL21lZGlhLW5ldHdvcmsvYXJ0aWNsZS9uZ_gC9NEekAPgA5gDjAaoAwHQBJBO4AQB0gUFEOeY9SWQBgGgBh_YBwDgBxs%2526num%253D0%2526cid%253DCAASEuRourlbFbnCT8eNqxFtsyqUSw%2526sig%253DAOD64_3LLauHW1d0ABDBcD-tH5-MgeQSpA%2526client%253Dca-pub-4830087483992392%2526adurl%253Dhttp%3A/register.theguardian.com/media/)

Indeed, many that work in the advertising industry are not convinced that consumers are about to embrace privacy tools. Among them is Martin McNulty, founder and CEO of digital agency [Forward3D](http://www.forward3d.com/). He believes that users generally get a good deal and value their online experience. “I think that, on the whole, people want better products and advertising. No one wants to get served bad advertising,” he says. “There are also a whole range of genuine benefits to online users trusting businesses with data, which are not always as well understood as the more publicised downsides. An exchange takes place. Data is exchanged for a faster, better, more relevant experience online.”

But McNulty is concerned about the [impact government legislation](http://www.theguardian.com/media-network/2015/jun/11/uk-tech-industry-threat-snoopers-charter-internet-surveillance) could have on user behaviour. With the UK government’s communications data bill being debated over the next year, he worries how this might affect his industry. “I am concerned with what the UK government is doing with the so-called ‘Snooper’s Charter’; I never thought the politics of privacy would come close to my day-to-day work of advertising. I think there’s a concern that this could get whipped up into a paranoia that could harm the advertising industry,” he says.

## Demographic bias

Other agency heads say it’s crucial for the industry to understand more about the impact different kinds of privacy tools on data. Henry Lewington, CEO of digital agency [Barracuda](http://barracuda.digital/), says users of privacy tools tend to be younger and more tech savvy types. “The impact of anonymous browsing has a demographic bias,” he says. “Sites which sell products or cater for a more technically knowledgeable audience tend to see higher rates of inaccuracy within the analytics data.”

Lewington says incognito browser sessions, where no third-party cookies are attached, mean the user will be marked as a new visitor. Those using anonymous search engines (DuckDuckGo), however, may be marked as referral traffic in Google analytics. Someone using a VPN will have their location masked, whereas someone using Tor will have their computer’s configuration completely hidden. “Marketers need to understand which tool is being used to understand its impact,” says Lewington.

So far, the impact on marketing data appears to be limited. It is also likely that many are using VPNs to bypass content restrictions rather than due to concerns over privacy. Tor usage is still very low and, again, might be used for specific purposes, rather than a day-to-day search enquires. However, what the web savvy do today we may all end up doing tomorrow, particularly if the new technologies are provided in a user-friendly format.

#  Let's learn the rules of the digital road before talking about a web Magna Carta

Neil Lawrence

Read more

## Invisible tracking

Those who have used Tor might be aware of the anonymous browser’s search engine of choice, [Disconnect.me](https://disconnect.me/). The software, designed by former Google engineers, is now available for mainstream users, with the company’s main product being a browser plug-in. Once installed, it acts like a VPN, but also blocks tracking requests from over 2,000 web analytics companies, social media sites and advertisers, at the same time highlighting who they are. “Disconnect allows users to block non-consensual invisible tracking that violates their privacy and puts them at risk for things like malware and identity theft,” says Casey Oppenheim, co-founder of Disconnect.me.

Oppenheim says he is not “opposed to advertising and marketing”, but says the business could make a big difference if the company’s user base continues to grow – it currently has about 10 million users. “Companies that engage in behaviour that violates user privacy and security may be harmed if our solution were to be adopted by the masses,” he says.

Certainly, there will be some battles ahead for the industry, and Disconnect.me looks set to be butting horns with the very biggest of beasts. At the time of writing, [Disconnect.me had filed an anti-trust law](http://www.zdnet.com/article/google-hit-with-ec-antitrust-complaint-after-booting-privacy-app-from-play-store/) suit in Europe against Google after it was omitted from its Play Store.

Oppenheim reckons that the battle over privacy and online anonymity is just getting going. “Privacy is definitely a battleground now, but is still small and will get much larger in the coming years. The reason is that when people find out the reality of how their privacy and security is being violated online, they really don’t like it. The people who argue for the status quo are almost invariably people who are directly making money from the status quo,” he says.

## **Anonymity on the Internet[**[**edit**](https://en.wikipedia.org/w/index.php?title=Anonymity&action=edit&section=8)**] Wikipedia**

*Further information:*[*Anonymous post*](https://en.wikipedia.org/wiki/Anonymous_post)

Most commentary on the Internet is essentially done anonymously, using unidentifiable pseudonyms. While these usernames can take on an identity of their own, they are frequently separated and anonymous from the actual author. According to the University of Stockholm this is creating more freedom of expression, and less accountability.[[8]](https://en.wikipedia.org/wiki/Anonymity#cite_note-8)[Wikipedia](https://en.wikipedia.org/wiki/Wikipedia) is collaboratively written mostly by authors using either unidentifiable pseudonyms or [IP address](https://en.wikipedia.org/wiki/IP_address) identifiers, although a few have used identified pseudonyms or their real names.

However, the Internet was not designed for anonymity: [IP addresses](https://en.wikipedia.org/wiki/IP_addresses) serve as virtual mailing addresses, which means that any time any resource on the Internet is accessed, it is accessed from a particular IP address. This address can be mapped to a particular [Internet Service Provider](https://en.wikipedia.org/wiki/Internet_Service_Provider) (ISP), and this ISP can then provide information about what customer that IP address was leased to. This does not necessarily implicate a specific individual (because other people could be using that customer's connection, especially if the customer is a public resource, such as a library), but it provides regional information and serves as powerful circumstantial evidence.

Anonymizing services such as [I2P](https://en.wikipedia.org/wiki/I2P) and [Tor](https://en.wikipedia.org/wiki/Tor_%28anonymity_network%29) address the issue of IP tracking. In short, they work by encrypting packets within multiple layers of encryption. The packet follows a predetermined route through the anonymizing network. Each router sees the immediate previous router as the origin and the immediate next router as the destination. Thus, no router ever knows both the true origin and destination of the packet. This makes these services more secure than centralized anonymizing services (where a central point of knowledge exists).[[9]](https://en.wikipedia.org/wiki/Anonymity#cite_note-9)

Sites such as [Chatroulette](https://en.wikipedia.org/wiki/Chatroulette) , [Omegle](https://en.wikipedia.org/wiki/Omegle) ,and [Tinder](https://en.wikipedia.org/wiki/Tinder) (which pair up random users for a conversation) capitalized on a fascination with anonymity. Apps like [Yik Yak](https://en.wikipedia.org/wiki/Yik_Yak) , [Secret](https://en.wikipedia.org/wiki/Secret_%28app%29) and[Whisper](https://en.wikipedia.org/wiki/Whisper_%28app%29) let people share things anonymously or quasi-anonymously whereas [Random](https://en.wikipedia.org/wiki/Random_%28application%29) lets the user to explore the web anonymously. Other sites, however, including [Facebook](https://en.wikipedia.org/wiki/Facebook)and [Google+](https://en.wikipedia.org/wiki/Google%2B), ask users to sign in with their legal names. In the case of Google+, this requirement led to a controversy known as the [nymwars](https://en.wikipedia.org/wiki/Nymwars).[[10]](https://en.wikipedia.org/wiki/Anonymity#cite_note-10)

The prevalence of [cyberbullying](https://en.wikipedia.org/wiki/Cyberbullying) is often attributed to relative Internet anonymity, due to the fact that potential offenders are able to mask their identities and prevent themselves from being caught. A principal in a high school stated that comments made on these anonymous site are "especially vicious and hurtful since there is no way to trace their source and it can be disseminated widely.[[11]](https://en.wikipedia.org/wiki/Anonymity#cite_note-11) "Cyberbullying, as opposed to general bullying, is still a widely-debated area of [Internet freedom](https://en.wikipedia.org/wiki/Internet_censorship) in several states.[[12]](https://en.wikipedia.org/wiki/Anonymity#cite_note-12)

As A. Michael Froomkin says: "*The regulation of anonymous and pseudonymous communications promises to be one of the most important and contentious Internet-related issues of the next decade".*[[13]](https://en.wikipedia.org/wiki/Anonymity#cite_note-13)[[14]](https://en.wikipedia.org/wiki/Anonymity#cite_note-14)

[David Chaum](https://en.wikipedia.org/wiki/David_Chaum) is called the Godfathers of anonymity and he has a claim to be one of the great visionaries of contemporary science. In the early 1980s, while a computer scientist at Berkeley, Chaum predicted the world in which computer networks would make mass surveillance a possibility. As Dr Wright explains: "David Chaum was very ahead of his time. He predicted in the early 1980s concerns that would arise on the internet 15 or 20 years later.".[[15]](https://en.wikipedia.org/wiki/Anonymity#cite_note-15) There are some people though that consider anonymity in internet being a danger for our society as a whole. David Davenport, an assistant professor in the Computer Engineering Department of Bilkent University in Ankara, Turkey, considers that by allowing anonymous Net communication, the fabric of our society is at risk.[[16]](https://en.wikipedia.org/wiki/Anonymity#cite_note-16) "A*ccountability requires those responsible for any misconduct be identified and brought to justice. However, if people remain anonymous, by definition, they cannot be identified, making it impossible to hold them accountable.*" he says.

**Is Anonymity Good or Bad?**[[17]](https://en.wikipedia.org/wiki/Anonymity#cite_note-17)

Anonymity and pseudonymity can be used for good and bad purposes. And anonymity can in many cases be desirable for one person and not desirable for another person. A company may, for example, not like an employee to divulge information about improper practices within the company, but society as a whole may find it important that such improper practices are publicly exposed. Good purposes of anonymity and pseudonymity:

* People dependent on an organization, or afraid of revenge, may divulge serious misuse, which should be revealed. Anonymous tips can be used as an information source by newspapers, as well as by police departments, soliciting tips aimed at catching criminals. Everyone will not regard such anonymous communication as good. For example, message boards established outside companies, but for employees of such companies to vent their opinions on their employer, have sometimes been used in ways that at least the companies themselves were not happy about [Abelson 2001].[[18]](https://en.wikipedia.org/wiki/Anonymity#cite_note-18) Police use of anonymity is a complex issue, since the police often will want to know the identity of the tipper in order to get more information, evaluate the reliability or get the tipper as a witness. Is it ethical for police to identify the tipper if it has opened up an anonymous tipping hotline?
* People in a country with a repressive political regime may use anonymity (for example Internet-based anonymity servers in other countries) to avoid persecution for their political opinions. Note that even in democratic countries, some people claim, rightly or wrongly, that certain political opinions are persecuted. [Wallace 1999][[19]](https://en.wikipedia.org/wiki/Anonymity#cite_note-19)[[20]](https://en.wikipedia.org/wiki/Anonymity#cite_note-20) gives an overview of uses of anonymity to protect political speech. Every country has a limit on which political opinions are allowed, and there are always people who want to express forbidden opinions, like racial agitation in most democratic countries.
* People may openly discuss personal stuff which would be embarrassing to tell many people about, such as sexual problems. Research shows that anonymous participants disclose significantly more information about themselves [Joinson 2001].[[21]](https://en.wikipedia.org/wiki/Anonymity#cite_note-21)
* People may get more objective evaluation of their messages, by not showing their real name.
* People are more equal in anonymous discussions, factors like status, gender, etc., will not influence the evaluation of what they say.
* Pseudonymity can be used to experiment with role playing, for example a man posing as a woman in order to understand the feelings of people of different gender.
* Pseudonymity can be a tool for timid people to dare establish contacts which can be of value for them and others, e.g. through contact advertisements.

There has always, however, also been a dark side of anonymity:

* Anonymity can be used to protect a criminal performing many different crimes, for example slander, distribution of child pornography, illegal threats, racial agitation, fraud, intentional damage such as distribution of computer viruses, etc. The exact set of illegal acts varies from country to country, but most countries have many laws forbidding certain "informational" acts, everything from high treason to instigation of rebellion, etc., to swindling.
* Anonymity can be used to seek contacts for performing illegal acts, like a pedophile searching for children to abuse or a swindler searching for people to rip off.
* Even when the act is not illegal, anonymity can be used for offensive or disruptive communication. For example, some people use anonymity in order to say nasty things about other people.

The border between illegal and legal but offensive use is not very sharp, and varies depending on the law in each country.[[22]](https://en.wikipedia.org/wiki/Anonymity#cite_note-22)

**Anonymous (group)**.[[23]](https://en.wikipedia.org/wiki/Anonymity#cite_note-23)

Anonymous (used as a mass noun) is a loosely associated international network of activist and hacktivist entities. A website nominally associated with the group describes it as "an internet gathering" with "a very loose and decentralized command structure that operates on ideas rather than directives".[[24]](https://en.wikipedia.org/wiki/Anonymity#cite_note-24) The group became known for a series of well-publicized publicity stunts and distributed denial-of-service (DDoS) attacks on government, religious, and corporate websites. An image commonly associated with Anonymous is the "man without a head" represents leaderless organization and anonymity.[[25]](https://en.wikipedia.org/wiki/Anonymity#cite_note-25)

## **Legal protection of anonymity[**[**edit**](https://en.wikipedia.org/w/index.php?title=Anonymity&action=edit&section=9)**]**

Anonymity is perceived as a right by many, especially the anonymity in the internet communications. The partial right for anonymity is legally protected to various degrees in different jurisdictions.

### United States**[**[**edit**](https://en.wikipedia.org/w/index.php?title=Anonymity&action=edit&section=10)**]**

The tradition of anonymous speech is older than the United States. Founders Alexander Hamilton, James Madison, and John Jay wrote the Federalist Papers under the pseudonym "Publius " and "the Federal Farmer" spoke up in rebuttal. The US Supreme Court has repeatedly[[26]](https://en.wikipedia.org/wiki/Anonymity#cite_note-26)[[27]](https://en.wikipedia.org/wiki/Anonymity#cite_note-27)[[28]](https://en.wikipedia.org/wiki/Anonymity#cite_note-28) recognized rights to speak anonymously derived from the[First Amendment.](https://en.wikipedia.org/wiki/First_Amendment_to_the_United_States_Constitution)

* The right for *anonymous political campaigning* was established in the [U.S. Supreme Court](https://en.wikipedia.org/wiki/U.S._Supreme_Court) decision in [*McIntyre v. Ohio Elections Commission*](https://en.wikipedia.org/wiki/McIntyre_v._Ohio_Elections_Commission) (1995) case: "Anonymity is a shield from the tyranny of the majority...It thus exemplifies the purpose behind the [Bill of Rights](https://en.wikipedia.org/wiki/United_States_Bill_of_Rights), and of the First Amendment in particular: to protect unpopular individuals from retaliation—and their ideas from suppression—at the hand of an intolerant society".[[29]](https://en.wikipedia.org/wiki/Anonymity#cite_note-29) The Supreme court explained that protecting anonymous political speech receives the highest protection however, this priority takes on new dimensions in the digital age.
* The right of individuals for "anonymous communication" was established by the decision in case *Columbia Insurance Company v. Seescandy.com, et al.* (1999) of the [U.S. District Court in the Northern District of California](https://en.wikipedia.org/w/index.php?title=U.S._District_Court_in_the_Northern_District_of_California&action=edit&redlink=1): "People are permitted to interact pseudonymously and anonymously with each other so long as those acts are not in violation of the law".[[30]](https://en.wikipedia.org/wiki/Anonymity#cite_note-30)
* The right of individuals for "anonymous reading" was established in the U.S. Supreme Court decision in *United States v. Rumely* (1953): "Once the government can demand of a publisher the names of the purchasers of his publications, the free press as we know it disappears. Then the spectre of a government agent will look over the shoulder of everyone who reads".[[31]](https://en.wikipedia.org/wiki/Anonymity#cite_note-31)

The pressure on anonymous communication has grown substantially after the 2001 terrorist attack on the World Trade Center and the subsequent new political climate. Although it is still difficult to oversee their exact implications, measures such as the US Patriot Act, the European Cybercrime Convention and the European Union rules on data retention are only few of the signs that the exercise of the right to the anonymous exchange of information is under substantial pressure.[[32]](https://en.wikipedia.org/wiki/Anonymity#cite_note-32)

A above-mentioned 1995 Supreme Court ruling in McIntyre v. Ohio Elections Commission reads:[[33]](https://en.wikipedia.org/wiki/Anonymity#cite_note-33) *"(...) rotections for anonymous speech are vital to democratic discourse. Allowing dissenters to shield their identities frees them to express critical minority views . . . Anonymity is a shield from the tyranny of the majority. . . . It thus exemplifies the purpose behind the Bill of Rights and of the First Amendment in particular: to protect unpopular individuals from retaliation . . . at the hand of an intolerant society."* However, anonymous online speech is not without limits. It is clearly demonstrated in a case from 2008, one in which the defendant stated on a law-school discussion board that two women should be raped, an anonymous poster’s comments may extend beyond free speech protections.[[34]](https://en.wikipedia.org/wiki/Anonymity#cite_note-34) In the case, a Connecticut federal court must apply a standard to decide whether the poster’s identity should be revealed. Significantly, however, there are several tests that the court could apply when considering this issue, some of which will be discussed here.[[35]](https://en.wikipedia.org/wiki/Anonymity#cite_note-35)[[36]](https://en.wikipedia.org/wiki/Anonymity#cite_note-36)[[*editorializing*](https://en.wikipedia.org/wiki/Wikipedia%3AManual_of_Style_%28words_to_watch%29#Editorializing)]

### European Union**[**[**edit**](https://en.wikipedia.org/w/index.php?title=Anonymity&action=edit&section=11)**]**

The right to internet anonymity is also covered by European legislation that recognizes the fundamental right to data protection, freedom of expression, freedom of impression. The European Union Charter of Fundamental Rights recognizes in Article. 8 (Title II: “Freedoms”)[[37]](https://en.wikipedia.org/wiki/Anonymity#cite_note-37) the right of everyone to protection of personal data concerning him.[[38]](https://en.wikipedia.org/wiki/Anonymity#cite_note-38) The right to privacy is now essentially the individual’s right to have and to maintain control over information about him.

### International legislation**[**[**edit**](https://en.wikipedia.org/w/index.php?title=Anonymity&action=edit&section=12)**]**

One of the most controversial international legal acts, regarding this subject is [Anti-Counterfeiting Trade Agreement (ACTA)](https://en.wikipedia.org/wiki/Anti-Counterfeiting_Trade_Agreement). As of February 2015, the treaty was signed -but not all ratified- by 31 states as well as the European Union. Japan was on 4 October 2012 the first to ratify the treaty. It creates an international regime for imposing civil and criminal penalties on Internet counterfeiting and copyright infringement. Although ACTA is intentionally vague, leaving signatories to draw precise rules themselves, critics say it could mean innocent travellers having their laptops searched for unlicensed music, or being jailed for carrying a generic drug. Infringers could be liable for the total loss of potential sales (implying that everyone who buys a counterfeit product would have bought the real thing). It applies to unintentional use of copyright material. It puts the onus on website owners to ensure they comply with laws across several territories. It has been negotiated secretively and outside established international trade bodies, despite EU criticisms.[[39]](https://en.wikipedia.org/wiki/Anonymity#cite_note-39)

[**Internet**](http://www.theguardian.com/technology/internet)

[The Observer](http://observer.theguardian.com/)

The worldwide web has made critics of us all. But with commenters able to hide behind a cloak of anonymity, the blog and chatroom have become forums for hatred and bile

 Websites are increasingly encouraging readers to leave comments, but with users able to hide behind aliases, often such attempts at discussion end in hate-filled bile and a mob mentality. Photograph: Sami Sarkis/Getty

[**Tim Adams**](http://www.theguardian.com/profile/timadams)

Saturday 23 July 2011 19.04 EDTLast modified on Friday 15 January 201612.02 EST

For a while after his first TV series was broadcast in 2009, comedian Stewart Lee was in the habit of collecting and filing some of the comments that people made about him on web pages and social media sites. He did a 10-minute Google trawl most days for about six months and the resultant collected observations soon ran to dozens of pages. If you read those comments now as a cumulative narrative, you begin to fear for Stewart Lee. A good third of the posts fantasised about violence being done to the comic, most of the rest could barely contain the extent of their loathing.

This is a small, representative selection:

*"I hate Stewart Lee with a passion. He's like Ian Huntley to me." Wharto15, Twitter
"I saw him at a gig once, and even offstage he was exuding an aura of creepy molesty smugness." Yukio Mishima, dontstartmeoff.com
"One man I would love to beat with a shit-covered cricket bat." Joycey, readytogo.net
"He's got one of those faces I just want to burn." Coxy, dontstartmeoff.com
"I hope stewart lee dies." Idrie, Youtube
"WHAT THE HELL! If i ever find you, lee, i promise i will, I WILL, kick the crap out of you." Carcrazychica, YouTube
"Stewart Lee is a cynical man, who has been able to build an entire carrer [sic] out of his own smugness. I hope the fucking chrones disease [sic] kills him." Maninabananasuit, Guardian.co.uk
"I spent the entire time thinking of how much I want to punch Stewart Lee in the face instead of laughing. He does have an incredibly punchable face, doesn't he? (I could just close my eyes, but fantasizing about punching Stewart Lee is still more fun than sitting in complete, stony silence.)" Pudabaya, beexcellenttoeachother.com*

Lee, a standup comedian who does not shy away from the more grotesque aspects of human behaviour, or always resist dishing out some bile of his own, does not think of himself as naive. But the sheer volume of the vitriol, its apparent absence of irony, set him back. For a few months, knowing the worst that people thought of him became a kind of weird compulsion, though he distanced himself from it slightly with the belief that he was doing his obsessive collating "in character". "Collecting all these up isn't something I would do," he suggests to me. "It is something the made-up comedian Stewart Lee would do, but I have to do it for him, because he is me…"

Advertisement

Distanced or not, Lee couldn't help but be somewhat unsettled by the rage he seemed to provoke by telling stories and jokes: "When I first realised the extent of this stuff I was shocked," he says. "Then it appeared to me that a lot of the things I was hated for were things I was actually trying to do; a lot of what people considered failings were to me successes. I sort of wrote a lot of series two of Stewart Lee's Comedy Vehicle with these comments in mind, trying to do more of the things people hadn't liked."

The "40,000 words of hate" have now become "anthropologically amusing" to him, he insists. "You can see a lot of them seem to be the same people posting the same stuff under different names in different places, and it is strange to see people you have known personally, whom you thought you had got on fine with at the time, abusing you under barely effective pseudonyms."

He's stopped looking these days, and never really tried to identify or confront any of his detractors. "I am slightly worried that some of them might be a bit insane and hope I haven't made myself or my family a target."

Lee is, of course, not alone in having this anonymous violent hatred directed toward him. On parts of the internet it has become pretty much common parlance. Do a quick trawl on the blog sites and comment sections about most celebrities and entertainers – not to mention politicians – and you will quickly discover comparable virtual rage and fantasised violence. Comedians seem to come in for more than most, as if taboo-breaking was taken as read, or the mood of the harshest baying club audience had become a kind of universal rhetoric. It's not quite heckling this, though, is it? A heckle requires a bit of courage and risk; the audience can see who is doing the shouting. Lee's detractors were all anonymous. How should we understand it then: harmless banter? Robust criticism? Vicious bullying?

Advertisement

The psychologists call it "deindividuation". It's what happens when social norms are withdrawn because identities are concealed. The classic deindividuation experiment concerned American children at Halloween. Trick-or-treaters were invited to take sweets left in the hall of a house on a table on which there was also a sum of money. When children arrived singly, and not wearing masks, only 8% of them stole any of the money. When they were in larger groups, with their identities concealed by fancy dress, that number rose to 80%. The combination of a faceless crowd and personal anonymity provoked individuals into breaking rules that under "normal" circumstances they would not have considered.

Deindividuation is what happens when we get behind the wheel of a car and feel moved to scream abuse at the woman in front who is slow in turning right. It is what motivates a responsible father in a football crowd to yell crude sexual hatred at the opposition or the referee. And it's why under the cover of an alias or an avatar on a website or a blog – surrounded by virtual strangers – conventionally restrained individuals might be moved to suggest a comedian should suffer all manner of violent torture because they don't like his jokes, or his face. Digital media allow almost unlimited opportunity for wilful deindividuation. They almost require it. The implications of those liberties, of the ubiquity of anonymity and the language of the crowd, are only beginning to be felt.

You can trace those implications right back to the genesis of social media, to pioneering Californian utopias, and their fall. The earliest network-groups had a sort of Edenic cast. One representative group was CommuniTree, which was set up as an open-access forum on a series of modem-linked computers in the 1970s when computers were just humming into life. For a while the group of like-minded enthusiasts ran on perfectly harmonious lines, respecting others, having positive and informed discussions about matters of shared relevance. At some point, however, some high school teenagers armed with modems accessed the open-access space and used it to trash and abuse the CommuniTree, taking free speech to uninhibited extremes that the pioneers had never wanted. The pioneers were suitably horrified. And eventually, after deciding that they could neither control the students through censorship, nor tolerate the space with them in it, they shut CommuniTree down.

This story has become almost folkloric among new media prophets, a sort of founding myth. It was one of the first moments when the possibilities of the new collective potential was tainted by anonymous lowest-common-denominator humanity, a pattern that has subsequently been repeated in pretty much all virtual communication. Barbarians, or "trolls" as they became known, had entered the community, ignoring the rules, shouting loudly, encouraging violence, spoiling it for everybody. Thereafter, anyone who has established a website or forum with high, or medium-high ideals, has had to decide how to deal with such anonymous destructive posters, those who got in the way of constructive debate.

Tom Postmes, a professor of social and organisational psychology at the universities of Exeter and Groningen in his native Netherlands, and author of Individuality and the Group, has been researching these issues for 20 years. "In the early years," he says, "this online behaviour was called flaming. And then that became institutionalised. Among friends, the people who engaged in this activity were actually quite jocular in intent but they were accountable to standards and norms that are radically different to those of most of their audience. Trolls aspire to violence, to the level of trouble they can cause in an environment. They want it to kick off. They want to promote antipathetic emotions of disgust and outrage, which morbidly gives them a sense of pleasure."

Postmes compares online aliases to the tags of graffiti artists: "Trolls want people to identify their style, to recognise them, or at least their online identity. But they will only be successful in this if an authority doesn't clamp down on them. So anonymity helps that. It's essentially risk-free."

Advertisement

There is no particular type of person drawn to this kind of covert bullying, he suggests: "Like football hooligans, they have family and live at home but when they go to a match the enjoyment comes from finding a context in which you can let go, or to use the familiar phrase 'take a moral vacation'. Doing this online has a similar characteristic. You would expect it is just normal people, the bloke you know at the corner shop or a woman from the office. They are the people typically doing this…"

Some trolls have become nearly as famous as the blogs to which they attach themselves, in a curious, parasitical kind of relationship. Jeffrey Wells, author of[Hollywood Elsewhere](http://www.hollywood-elsewhere.com/), is a former columnist on the LA Times who has been blogging inside stories about movies for 15 years. For the last couple of years his gossip and commentary has been dogged by the invective of a character called LexG, whose 200-odd self-loathing and wildly negative posts recently moved Wells to [address him directly](http://www.hollywood-elsewhere.com/2010/08/lexg_stays_but.php): "The coarseness, the self-pity and the occasional eye-pokes and cruel dismissiveness have to be turned down. Way down. Arguments and genuine disdain for certain debaters can be entertaining, mind. I'm not trying to be Ms Manners. But there finally has to be an emphasis on perception and love and passion and the glories of good writing. There has to be an emphasis on letting in the light rather than damning the darkness of the trolls and vomiting on the floor and kicking this or that Hollywood Elsewhere contributor in the balls…"

When I spoke to Wells about LexG, he was philosophical. "Everybody on the site writes anonymously, except me," he says. "If they didn't I think it would cause them to dry up. This place is like a bubble in which you can explode, let the inner lava out. And, boy, is there a lot of lava."

He has resisted insisting that people write under their own name because that would kill the comments instantly. "Why would you take that one in 100 chance that your mother or a future employer will read what you were thinking late one night a dozen years ago if you didn't have to?" For haters, Wells believes, anonymity makes for livelier writing. "It's a trick, really – the less you feel you will be identified, the more uninhibited you can be. At his best LexG really knows how to write well and hold a thought and keep it going. He is relatively sane but certainly not a happy guy. He's been doing this a couple of years now and he really has become a presence; he does it on all the Hollywood sites."

Have they ever met?

"Just once," Wells says. "I asked him to write a column of his own, give him a corner of the site, bring him out in the open." LexG didn't want to do it, he seemed horrified at the prospect. "He just wanted to comment on my stuff," Wells suggests. "He is a counter-puncher, I guess. The rules on my site remain simple, though. No ugly rancid personal comments directed against me. And no Tea Party bullshit."

The big problem he finds running the blog is that his anonymous commenters get a kind of pack mentality. And the comments quickly become a one-note invective. As a writer Wells feels he needs a range of emotion: "I also do personal confession or I can be really enthusiastic about something. But the comments tend to be one colour, and that becomes drab. It's tougher, I guess, to be enthusiastic, to really set out honestly why something means something to you. It takes maybe twice as long. I can run with disdain and nastiness for a while but you don't want to always be the guy banging a shoe on the table. Like LexG. I mean it's not healthy, for a start…"

Wells does his own marshalling of the debate, somewhat like the bartender of a western saloon. Other sites – including our own [Comment is Free](http://www.theguardian.com/us/commentisfree) – employ moderators to try to keep trolls in line, and move the debate on. A young journalist called Sarah Bee was for three years the moderator on seminal techie news and chat forum [the Register](http://www.theregister.co.uk/). She started as a sub-editor but increasingly devoted her time to looking after the "very boisterous" chat on the site. She has no doubt that "anonymity makes people bolder and more arsey, of course it does. And it was quite a politically libertarian crowd, so you get people expressing things extremely stridently, people would disagree and there would often be a lot of real nastiness." She was very liberal as far as moderating went, she thinks, with no real hard and fast rules, except, perhaps, for "a ban on prison-rape jokes, which came up extremely often".

Advertisement

Every once in a while, however, the mood would get "very ugly" and she would try to calm things down and remonstrate with people. "I would occasionally email them – they had to give their email addresses when registering for the site – to say, 'Even though you are not writing under your real name, people can hear you.'" In those instances, strangely, she suggests, most people were incredibly contrite when contacted. It was like they had forgotten who they were. "They would send messages back saying, 'Oh, I'm so sorry', not even using the excuse of having a bad day or anything like that. It is so much to do with anonymity…"

Bee became known as the Moderatrix – "all moderators have an implicit sub-dom relationship with their site" – though she was just about the only person in the comment section who used her own name. "There was a lot of misogyny and casual sexism, some pretty off-colour stuff. I would get a few horrible emails calling me a cunt or whatever," she says, "but that didn't bother me as much as the day-to-day stuff, really."

The day-to-day stuff was, though, "like being in another world. It got really wearying. I would go home sometimes and just sigh and wonder about it all."

She is keen to say that the Register itself she thought a great thing, and loved the idea of working there, but being Moderatrix eventually got her down. "A hive mind sets in," she suggests. "Just occasionally good sense would prevail but then there is that fact that arguments on the internet are literally never over. You moderate a few hundred comments a day, and then you come in the next morning and there are a few hundred more waiting for you. It's Sisyphean."

In the end she needed a change. She's in another "community management" job now, dealing through Facebook, which is a relief because "it removes anonymity so people are a lot more polite". When she retired Moderatrix [she did a goodbye](http://www.theregister.co.uk/2011/06/30/moderatrix_off/)and got 250 comments wishing her well. She doesn't miss it, though. "Just occasionally I would let a stream of the most offensive things through, just to let people know how those things looked in the world… People would realise for a bit. But then the old behaviours would immediately set in. The thing any moderator will tell you is that every day is a new day and everything repeats itself every day. It is not about progress or continuity…"

There are many places, of course, on the internet where a utopian ideal of "here comes everybody" prevails, where the anonymous hive mind is fantastically curious and productive. A while ago I talked to Jimmy Wales, the founder of Wikipedia, about some of this, and asked him who his perfect contributor was. "The ideal Wikipedian, in my mind, is someone who is really smart and really kind," he said, without irony. "Those are the people who are drawn into the centre of the group. When people get power in these communities, it is not through shouting loudest, it is through diplomacy and conflict resolution."

Within this "wikitopia" there were, too, though, plenty of Lord of the Fliesmoments. The benevolent Wiki community is plagued by "Wikitrolls" – vandals who set out to insert slander and nonsense into pages. A policing system has grown up to root out troll elements; there are well over 1,000 official volunteer "admins", working round the clock; they are supported in this work by the eyes and ears of the moral majority of "virtuous" Wikipedians.

"When we think about difficult users there are two kinds," Wales said, with the same kind of weariness as Moderatrix. "The easy kind is someone who comes in, calls everyone Nazis, starts wrecking articles. That is easy to deal with: you block them, and everyone moves on. The hard ones are people who are doing good work in some respects but are also really difficult characters and they annoy other people, so we end up with these long intractable situations where a community can't come to a decision. But I think that is probably true of any human community."

Advertisement

Wales, who has conducted perhaps the most hopeful experiment in human collective knowledge of all time, appears to have no doubt that the libertarian goals of the internet would benefit from some similar voluntary restraining authority. It was the case of the blogger Kathy Sierra that caused Wales and others to propose in 2007 an unofficial code of conduct on blog sites, part of which would outlaw anonymity. Kathy Sierra is a programming instructor based in California; after an online spat on a tech-site she was apparently randomly targeted by an anonymous mob that posted images of her as a sexually mutilated corpse on various websites and issued death threats. She wrote on her own blog: "I'm at home, with the doors locked, terrified. I am afraid to leave my yard, I will never feel the same. I will never be the same."

Among Wales's suggestions in response to this and other comparable horror stories of virtual bullying was that bloggers consider banning anonymous comments altogether, and that they be able to delete comments deemed abusive without facing accusations of censorship. Wales's proposals were quickly shot down by the libertarians, and the traffic-hungry, as unworkable and against the prevailing spirit of free-speech.

Other pioneering idealists of virtual reality have lately come to question some of those norms, though. Jaron Lanier is credited with being the inventor of virtual worlds. His was the first company to sell virtual reality gloves and goggles. He was a key adviser in the creation of avatar universe Second Life. His recent book, You Are Not a Gadget, is, in this sense, something of a mea culpa, an argument for the sanctity of the breathing human individual against the increasingly anonymous virtual crowd. "Trolling is not a string of isolated incidents," Lanier argued, "but the status quo in the online world." He suggested "drive-by anonymity", in which posters create a pseudonym in order to promote a particularly violent point of view, threatened to undermine human communication in general. "To have substantial exchange, you need to be fully present. That is why facing one's accuser is a fundamental right of the accused."

We rightly hear a great deal about the potential of social media and websites to spread individual freedom, as evidenced during the Arab spring and elsewhere. Less is written about their capacity to reinforce pack identities and mob rule, though clearly that is also part of that potential.

Social psychologist Tom Postmes has been disturbed by the coarsening of debate around issues such as racial integration in his native Netherlands, a polarisation that he suggests has grown directly from the fashionable political incorrectness of particular websites where anonymity is guaranteed. "There is some evidence to suggest that the mainstream conservative media even cuts politically correct or moderate posts from websites in favour of the extremes," he says. "The tone of the public debate around immigration has diminished enormously in these forums."

One effect of "deindividuation" is a polarisation within groups in which like-minded people typically end up in more extreme positions because they gain credibility by exaggerating loosely held prejudices. You can see that in the bloggers trying to outdo one another with pejoratives about Stewart Lee. This has the effect of shifting norms: extremism becomes acceptable. As Lanier argues: "I worry about the next generation of young people around the world growing up with internet-based technology that emphasises crowd aggregation… will they be more likely to succumb to pack dynamics when they come of age?" The utopian tendency is to believe that social media pluralises and diversifies opinion; most of the evidence suggests that it is just as likely, when combined with anonymity, to reinforce groupthink and extremism.

A lot of this comes down to the politics of anonymity, a subject likely to greatly exercise the minds of legislators as our media becomes increasingly digitised, and we rely more and more on mostly unaccountable and easily manipulated sources – from TripAdvisor to Twitter feeds to blog gossip – for our information.

One simple antidote to this seems to rest in the very old-fashioned idea of standing by your good name. Adopt a pseudonym and you are not putting much of yourself on the line. Put your name to something and your words are freighted with responsibility. Arthur Schoepenhauer wrote well on the subject 160 years ago: "Anonymity is the refuge for all literary and journalistic rascality," he suggested. "It is a practice which must be completely stopped. Every article, even in a newspaper, should be accompanied by the name of its author; and the editor should be made strictly responsible for the accuracy of the signature. The freedom of the press should be thus far restricted; so that when a man publicly proclaims through the far-sounding trumpet of the newspaper, he should be answerable for it, at any rate with his honour, if he has any; and if he has none, let his name neutralise the effect of his words. And since even the most insignificant person is known in his own circle, the result of such a measure would be to put an end to two-thirds of the newspaper lies, and to restrain the audacity of many a poisonous tongue."

The internet amplifies Schopenhauer's trumpet many times over. Though there are repressive regimes when anonymity is a prerequisite of freedom, and occasions in democracies when anonymity must be preserved, it is clear when those reservations might apply. Generally, though, who should be afraid to stand up and put their name to their words? And why should anyone listen if they don't?

Entrepreneur

# Internet Users Want to Be Invisible. And They Fear Advertisers More than the Government

The uproar over the surveillance practices of the National Security Agency has taken center stage in Washington, but for the majority of internet users, advertisers are more feared than the government, according to a new survey from the Pew Research Center.

Almost 9 in 10 internet users, or 86 percent of Pew survey respondents, report having taken steps to wipe away or hide their digital whereabouts. Practices include everything from clearing one's browser history to using a public computer to be able to browse anonymously. And 55 percent of survey respondents have taken actions those actions to clear their internet history to avoid specific people, organizations or the government, the report says.

**Related:**[**How to Avoid Getting Hacked (Infographic)**](http://www.entrepreneur.com/article/227949)

Unsurprisingly, internet users say their top threat [online is hackers and criminals](http://www.entrepreneur.com/security/index.html). Their second most avoided foe are advertisers, with 28 percent of survey respondents saying they have attempted to hide from advertisers online. Nineteen percent of users said they wanted to avoid people from their past and specific friends. Meanwhile, only 5 percent of respondents attribute their attempts to be covert on the internet to avoiding the government.

Even as they take steps to cover their digital tracks, however, many internet users know that in this age of hacking, nothing is really ever gone.

**Related:**[**Surge in Mobile Banking Creates a Security Gap That's a 'Wild West' for Fraudsters**](http://www.entrepreneur.com/article/227813)

“Users clearly want the option of being anonymous online and increasingly worry that this is not possible,” Lee Rainie, director of the Pew Research Center’s Internet said in a statement. “Their concerns apply to an entire ecosystem of surveillance. In fact, they are more intent on trying to mask their personal information from hackers, advertisers, friends and family members than they are trying to avoid observation by the government.”’



Internet users fret about their personal identity being uncovered online because the chances are decently high that either they or somebody they know have suffered a consequence. Here is a look at what survey respondents report having suffered:

* 21 percent of internet users have had an email or social networking account violated or taken over
* 12 percent have been stalked or harassed online
* 11 percent have personal information stolen, including such their Social Security Number, credit card, or bank account information
* 6 percent have lost money after being the victim of an online scam
* 6 percent have had their reputation damaged because of an online faux pas
* 4 percent have experienced physical danger as a result of online activity

The [survey from Washington, D.C.-based Pew Research Center](http://pewinternet.org/Reports/2013/Anonymity-online/Summary-of-Findings/Key-findings.aspx)included responses from 792 internet users, all of whom were surveyed between July 11 and 14 on the telephone by the Princeton Survey Research Associates.

# The Marketer February 3, 2016

# Who Do Great Britain's Internet Users Trust with Data?

## **Almost all internet users are concerned about privacy**

February 3, 2016 | [Retail & Ecommerce](http://www.emarketer.com/topics/Retail-Ecommerce/1047)

Virtually all internet users in Great Britain are worried about their digital privacy—but most also think they know what to do to protect themselves.



0

A January 2016 survey by [TRUSTe](http://www.truste.org/), [Ipsos](http://www.ipsos.com/) and [National Cyber Security Alliance](http://www.staysafeonline.info/) reveals that 95.5% of internet users in Great Britain worry about digital privacy, and not passively, either—87% of those surveyed are aware of activities that are related to data privacy as well as activities that could be done to protect digital privacy. What’s more, only 13% say they would use a website even if they did not trust the company or service to handle their personal information responsibly. But who do they trust to do that?

Healthcare providers are perceived as the most trustworthy users of consumer data; 72% of respondents trust them with personal data. Another 66% find financial organizations able to handle their personal data with care. But social media and advertising firms don”t fill internet users with much confidence: 32% trust social networks, and only 19% trust advertisers.



How, then, do internet users in Great Britain want to control usage of their personal data? One in two surveyed say they’d like to determine who has access to their information, and another 47% would like to dictate how that information is used. Only 29% say they want the ability to delete collected information—this answer, however, may be influenced by the 50% who say they want to control who gets personal information to begin with.

It’s no surprise nearly everyone is concerned about what companies do with their personal data. More notable is that Great Britain’s internet users are educated about the issue, and are looking to actively control their information.

- See more at: <http://www.emarketer.com/Article/Who-Do-Great-Britains-Internet-Users-Trust-with-Data/1013544#sthash.hX4jjyoL.dpuf>

<http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/>

<http://www.pewinternet.org/2014/11/12/what-americans-think-about-privacy/>

<http://www.pewinternet.org/2013/05/21/teens-social-media-and-privacy-3/>