The Privacy Surgeon

Predictions for Privacy

A report on the issues and trends that will dominate the privacy landscape in 2013

Compiled by Simon Davies, PrivacySurgeon.org

Published by LSE Enterprise, the London School of Economics

January 2013

www.privacysurgeon.org

Published by LSE Enterprise

Contents

About

Predictions for Privacy was compiled by Simon Davies, a leading advocate and privacy specialist with more than 25 years of experience in the field. He is widely acknowledged as one of the world's foremost privacy experts and is one of the pioneers of the international privacy arena. Davies is Founder of Privacy International and has conducted research, outreach and campaigns in more than fifty countries. He now manages the education and blogging resource www.privacysurgeon.org

This report is published by LSE Enterprise - the commercial arm of the London School of Economics. LSEE specializes in executive education and consulting and is the body that manages the professional interface with LSE academic departments to enable commercial application of the LSE's expertise and intellectual resources. Davies is an Associate Director of LSE Enterprise.

Summary

This aim of this report is to establish a framework to understand the dynamics that might shape public policy and public opinion in the privacy realm. The project surveyed 181 privacy specialists from 19 countries to identify the key trends and issues that are likely to dominate the privacy landscape over the coming year.

2013 is likely to eclipse the previous year's record exposure of privacy issues. Respondents identified a number of key trends that are set to drive media reporting and political activity beyond the level of past years. More aggressive action by companies to monetise personal information through advertising will inevitably fuel controversy, while consolidation of markets such as social networking may induce emerging players to engage dangerous privacy practices. However in many respects it is becoming clear that the exploitation of personal information by governments and corporations has already tested the limits of public tolerance.

Respondents identified ten key privacy issues for 2013

1. Mobile apps
2. Mobile geo-location
3. Data aggregation
4. Online advertising
5. Data protection reform
6. Big Data
7. Face recognition systems
8. Government surveillance systems
9. Health data for private sector us
10. Compulsory website ownership registration and verification

The five most influential privacy themes identified by respondents for 2013 are:

1. Data aggregation
2. Regulatory changes
3. Consent
4. Transparency
5. Privacy of children and young people

Background

In August 2012 the Privacy Surgeon launched a survey[1] to determine the privacy issues that are likely to reach prominence in 2013. This exercise will be repeated annually.

The aim of the project was to establish a framework to identify the likely trends and events that would shape public policy and media reporting in the privacy realm over the coming year. One of the principal objectives was to construct an integrated picture of this complex field to reach a better understanding of the dynamics of privacy issues.

The work began with a consultation in which privacy professionals, ITC experts, legal specialists, regulators and specialist media were invited to submit their views. More than 400 people were directly approached and the call was also circulated on various specialist lists, including Privacy International, the European Digital Rights Initiative (EDRi), the Berlin Working Group on Telecommunications and the Foundation for Information Policy Research (FIPR).

This outreach resulted in 181 responses from 19 countries. The breakdown of responses is as follows:

Legal professionals	28
Media professionals	19
Political advisers	4
Senior government managers	21
Private sector privacy officers	26
Independent consultants	13
Civil society	24
Regulators	12
Academic experts	26
Other	8
Total	**181**

It was not the intention of this survey to become a “wish list” of issues, but rather, an objective expert view on the likely future shape of privacy issues for the coming year. One of the more interesting challenges facing this project was to distinguish the specific professional interests of respondents from a (perhaps) more objective perspective. In this way the assessment of

[1] http://www.privacysurgeon.org/blog/incision/polling-commences-to-identify-the-key-privacy-issues-of-the-coming-year/

responses focused on the issues that "would" be prominent, rather than those that "should" be prominent.

Overview of key trends

In many respects 2012 was a landmark year for privacy. Europe accelerated its process of data protection reform while countries throughout South America and Asia began introducing legislation to protect personal privacy. Media reporting of privacy issues reached an all-time highpoint as the topic moved further toward becoming an entrenched element of mainstream journalism.

However 2012 was also noteworthy because of a litany of negative press reports of privacy issues, ranging from increased government data surveillance[2] and poor privacy practices of corporations to the privacy fallout from the Petraeus probe.[3]

Responses to this survey indicate that 2013 is likely to eclipse the previous year's exposure. Respondents identified a number of key trends that are set to drive media reporting and political activity beyond the level of previous years. More aggressive action by companies to monetise personal information through advertising will inevitably fuel controversy, while consolidation of markets such as social networking may induce emerging players to engage dangerous privacy practices. However in many respects it is becoming clear that the exploitation of personal information by governments and corporations has already tested the limits of public tolerance.

The survey, however, reveals an interesting dichotomy. While there is a clear trend toward stronger and more inclusive privacy regulation - together with some noteworthy privacy-enhancing design and engineering developments - there is an equally strong trend toward information practices and corporate strategies that defy or circumvent regulation. 2012 revealed the extent to which the business models of major information companies often collided head-on with good privacy standards. 2013 is likely to be the year when that conflict is placed under the microscope.

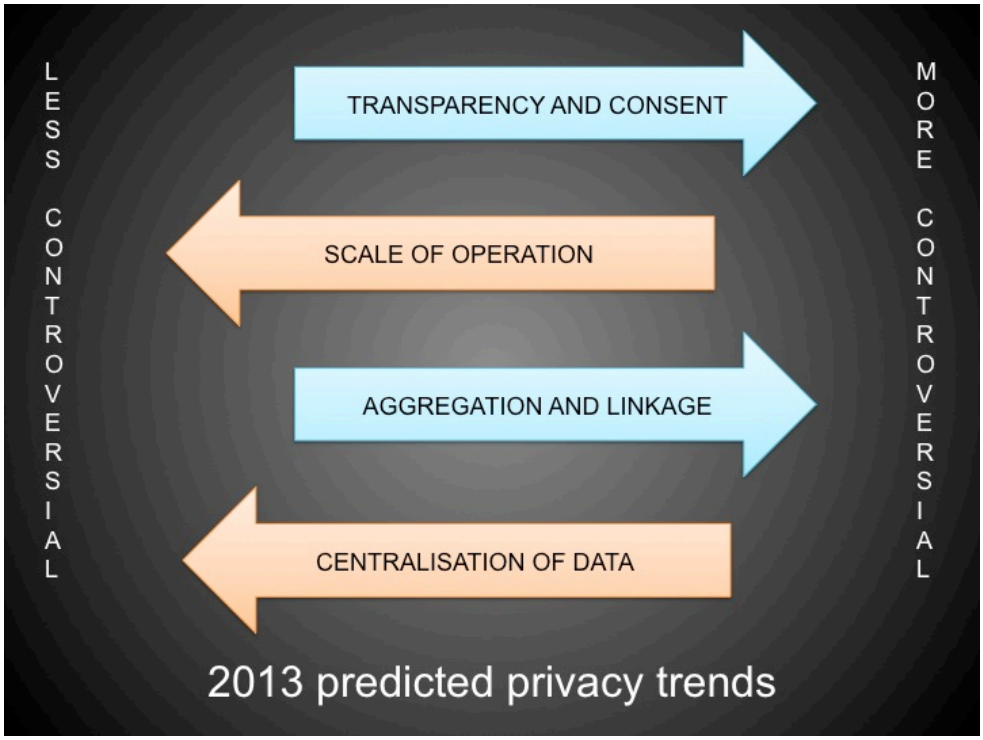
Negative media coverage of privacy issues over the actions of global corporations such as Google and Facebook reached a peak in 2012, with no slowdown in sight. However, media reporting of issues that respondents felt were generally positive - for example Microsoft's default enabling of the *Do*

---

2 http://www.slate.com/blogs/future_tense/2012/12/13/national_counterterrorism_center_s_massive_new_surveillance_program_uncovered.html?fb_action_ids=10151216593094102&fb_action_types=og.likes&fb_source=other_multiline&action_object_map={%2210151216593094102%22%3A457377207653622}&action_type_map={%2210151216593094102%22%3A%22og.likes%22}&action_ref_map=[]

3 http://tech.fortune.cnn.com/2012/12/17/petraeus-privacy-act/

Not Track anti-tracking feature and key positive developments in privacy engineering - received scant coverage. The resulting bias has triggered a possible drift in public consciousness toward a passive acceptance that exploitation of personal information is simply an unavoidable fact of life. In this scenario legislation is incapable of guaranteeing rights, industry self-regulation is illusory and technical measures are peripheral.



While this consciousness may suit the short-term interests of some less ethical players in the market, such an outlook does not engender the level of trust that is required to fuel emerging products and services that require a high degree of certainty of security and privacy.

Nonetheless, the respondents overwhelmingly felt that the coming year would witness a shift toward more effective activism by consumers, media and regulators. In sympathy with this view the *Economist* magazine began the year with an article[4] comprehensively arguing that the activism landscape has evolved substantially in recent times. Indeed the last two major privacy issue of 2012 – the sweeping changes to Instagram's terms and conditions and the ITU's proposed global Internet restrictions - triggered an immediate and influential global backlash, indicating that in at least some respects sensitivity on privacy issues had reached a notable peak. The diversification of privacy activism combined with the rapid growth of organizations such as the European Digital Rights Initiative (EDRi) stand in testimony to this shift.

[4] http://www.economist.com/news/briefing/21569041-can-internet-activism-turn-real-political-movement-everything-connected

Many respondents also felt that the spread of privacy regulation would exert a generally positive effect over the coming year. This regulatory expansion is substantial, as the following summary provided by Noriswadi Ismail of Quotient Consulting neatly summarises:

> *Three ASEAN member states passed omnibus data protection legislation. The Malaysian Personal Data Protection Act (PDPA) 2010, passed in 2010 will be enforced by 1st January 2013. Republic Act No. 10173 (known as Data Privacy Act 2012) passed on 15th August 2012, is expected to be enforced by 2013 once the National Privacy Commission has finalised the rules and regulations of the Act. On 3rd December 2012 the Singapore Personal Data Protection Act 2012 was passed, enforceable after a transition period of 12 months and - once the data protection rules come into force - after 18 months. Of these, the PDPA 2010 and PDPA 2012 only apply to commercial transactions/private sectors. In 2013 Indonesia shall be revisiting its pending data protection bill.*

Despite substantial deficiencies in these laws the trend is likely to trigger increased regulatory activity across the region over the coming year – an outcome that is becoming evident in Canada and parts of Europe.

Although 2013 began with a controversial FTC antitrust ruling[5] on an investigation into Google's activities there are indications that this outcome is an exceptional case. Respondents reported that in many regions increased scrutiny of regulators by activists is resulting in more assertive regulatory action on privacy issues. European regulators became more aggressive over the activities of companies such as Google,[6] while the German state of Schleswig-Holstein recently declared that Facebook's requirement for the use of real identities was illegal.[7]

Despite this overall shift to stronger regulation and more effective activism, many respondents expressed concern that privacy will be characterized as a "lost cause" that defies an inevitable shift to total information awareness by governments and corporations.

Anne Cavoukian, Ontario's Privacy & Information Commissioner highlighted this concern in her submission to this report:

> *One of the biggest issues I foresee for the future of privacy is dispelling the myths that presently abound and ensuring that perception doesn't become reality. it seems that every day I encounter someone saying -- "there can be no more privacy because of the growth of online social*

[5] http://www.nytimes.com/2013/01/07/technology/googles-rivals-say-ftc-antitrust-ruling-missed-the-point.html?_r=0
[6] http://www.guardian.co.uk/technology/2012/oct/15/google-privacy-policy
[7] http://www.spiegel.de/netzwelt/netzpolitik/klarnamen-pflicht-weichert-stellt-facebook-ultimatum-a-873411.html

media", or "privacy is dead because everyone is connecting wirelessly through mobile devices" or something along those lines predicting the death of privacy. I know for a fact that we can have privacy along with all of these new developments through Privacy Enhancing Technologies, Privacy by Design, Biometric Encryption, and much more, but I fear that the headlines will prevail and people will simply give up on privacy because of their flawed views.

Such responses stressed that while there is an undeniable shift toward technological solutions and privacy innovation, the public mood sometimes demonstrates a sense of inevitability of the surveillance state.

The key triggers for public concern

Respondents consistently identified five “triggers” that they believed would permeate the spectrum of key issues and that would act as a lightning rod for public concern.

Two interlinking elements at the top of this list are transparency and consent (or - more accurately - secrecy and non-consent). Respondents believed that even when consumers were unconcerned about consent to process personal information, they would increasingly react with anger when such operations are conducted without transparency. This does not necessarily mean that consumers would be content with mere notification of this processing. There appears to be an emerging expectation that organizations should be more responsive to - and interactive with - the people who are affected by the processing.

Alongside these dynamics is an apparent relaxation of concern over two formerly controversial aspects – the scale of operation of large companies (the amount of data collected) and the centralization of data. It has been proposed that many people have become so accustomed to reading about huge storage and processing figures within cloud or social networking services that they have become somewhat desensitized to scale.

However there was a considerable amount of concern expressed by respondents on the subject of data aggregation – the bringing together of various strands of a consumer’s activities.

One European Commission official responded:

I feel that the trend toward merging all the different activities of users into a detailed profile will in time create a real breakdown of trust in online services, and these concerns are already registering in media and political circles. There should be a limit to the claim that good customer service is dependant on making every activity linkable and

known to the company. Aggregation of this sort will imperil trust in privacy protections.

While aggregation has been in existence as a process for many years (it has its roots in the 1970s with the process of data matching[8]) it has perhaps been only in recent times that consumers have understood that data aggregation can form a foundation for privacy violation on an industrial scale.

One apparent reason why data aggregation worried respondents is that the online industry confronted this issue in a very public way in March 2012 when Google unveiled plans to aggregate data for its users across all sixty products and services. To do so, the company revised its privacy statement to allow saturation aggregation of individual user data and the monetization of that data through ad sales. While this strategy has been witnessed in other parts of the industry, European privacy regulators determined that the Google policy change violated European privacy laws.

Some concern was expressed that Google has adopted a "crash or crash through" strategy to test the limits of regulation (particularly in Europe), rather than pursuing synergy with regulation. Again, while this strategy is not new, it should be viewed with renewed anxiety in the light of Google's dominant position in several markets.

One interpretation of the survey results is that the continued intense negative coverage of Google could create a "negative centre of gravity" that could destabilize overall confidence in the ability of online services and data processors to respect personal privacy. Google is tipped to be the most controversial brand of 2013, and as a market leader this controversy could spark a crisis of consumer confidence.

Similar concerns were raised about the overall damping effect of Facebook coverage. Until recently it was felt that – in contrast to Google's almost ubiquitous portfolio - Facebook's ambit was limited to a relatively narrow spectrum of online activity and thus the corrosive influence of continuing negative coverage would be limited. However in recent weeks there has been a broadening of concern over new Facebook policies and services such as Search[9] and Identity[10]. Facebook's work on the "next generation" of targeted advertising[11] is one reason why that topic reached the Red List of issues in this report.

---

[8] http://www.rogerclarke.com/DV/MatchIntro.html

[9] http://www.thenation.com/blog/172459/why-graph-search-could-be-facebooks-largest-privacy-invasion-ever#

[10] http://www.itproportal.com/2013/01/28/facebook-demands-photo-id-as-part-of-new-verification-process/

[11] http://www.businessinsider.com/facebooks-plan-to-kill-the-tracking-cookie-2013-1

Because of these concerns anxiety over the privacy of the data of children and young people will accelerate in 2013. Will Roebuck of E RADAR observed:

> *I think one of the key issues around privacy is more education, particularly for younger people on the perils of giving too much information away on social media and networking websites. There is now a blurred line between information given to friends and to business/professional colleagues. I'm hearing more stories about perspective employers visiting the online profiles of candidates before making job offers. Whether you agree or not with the ethics of this, organisations do have duties of due diligence in order to protect investors and their brand. Social media is an opportunity to facilitate this. Of course, there are also the bigger issues around electronic crime and identity theft which we need to deal with by educating online users in general.*

The Red List: ten key issues for 2013

Many responses from contributors were both complex and wide-ranging. More than two hundred privacy topics were submitted, many of which were set in the context of converging themes and trends. Some of these topics cut across several fields of professional interest, while others were so novel that they defied categorization.

For example Jennifer Stoddart, Federal Privacy Commissioner of Canada, submitted the following ten topics that she felt would be significant in the coming year:

- Privacy in an age of government transparency
- Personal responsibility for privacy violations
- Emerging common law private rights of action for victims of privacy violations
- The intersection between payments and privacy in the digital age
- Privacy implications of youth targeted as direct consumers
- Absence of privacy accountability frameworks
- The crosswalk between law enforcement authorities and private sector data holders
- Vulnerability of cyber-security
- Increased citizen awareness of privacy risks
- Ubiquitous mobile devices – changing how we interact in the public/private divide

In many respects every one of these aspects deserves to be a priority, but as this report sought primarily to discover popular converging views, several of the above topics did not make it to either the red or amber list. The fact that a topic did not make the “hot” lists should not imply it is any less significant; it

merely indicates that the topic is not seen as a key trigger for public or policy action in the coming year.

The top ten issues are:

Mobile apps

This topic was the front-runner. Although some action is currently being taken to improve privacy standards across the sector[12] there are serious concerns that self regulation will be largely ineffective and that mobile network providers will be unable to ensure a high standard of protection against the misuse of personal information.

Mobile geo-location

Many respondents felt that this "new frontier" for mobile services will become exceptionally dangerous terrain for privacy, and coupled with data aggregation (see below) mobile networks and devices will create a granular and real-time tracking and profiling mechanism across entire populations.

Data aggregation

As outlined in the above section on trends, many respondents felt that the process of aggregation – either by directly merging different data streams or creating data conduits across disparate services – would be a significant trigger for public concern in 2013.

Online advertising

This aspect intersects with many of the Red List issues, particularly search and geo-location. Coupled with the perception of compounding failure over *Do Not Track* and other initiatives many respondents felt that increased levels of granular intrusion into the online activities of users would be a major issue of concern over the coming year. Recent polling[13] suggests that there is already a considerable level of public concern over tracking.

Data protection reform

As Europe prepares to revamp its privacy protection framework through the new data protection regulation there will be increased concern over the activities of lobbyists representing interests that seek

[12] http://www.insideprivacy.com/united-states/rep-johnson-releases-discussion-draft-of-mobile-app-privacy-bill-following-ntias-8th-meeting-concern/

[13] http://www.informationweek.com/windows/security/microsoft-finds-people-want-more-privacy/240146932

to undermine those protections.[14] This concern parallels anxiety over the perceived imbalance in negotiations between the EU and the US on security and policing arrangements.

Big Data

Although respondents suggested that the public was becoming less concerned about issues of scale and size of data holdings, the concept of "Big Data" is likely to attract significant interest, particularly in the context of data linkage and government intrusion through the compulsory acquisition of this information.

Face recognition

Face recognition will become a controversial issue in 2013 as the technology moves into the mainstream of search and apps development. There are significant privacy issues associated with this technique, particularly with regard to search and tagging. Face recognition has already become a standard feature in many technologies and services.

Government surveillance systems

While the activities of corporations dominated predictions for the coming year there was a high degree of certainty that intrusion by government would continue to generate considerable anxiety across the world. This will particularly be the case in the US[15] and the UK[16], where government is pushing the frontiers of surveillance of personal activities. Mark Hughes of the Institute for the Study of Privacy Issues explains that the concern would stem from the use for surveillance of "interconnected databases originally intended (and justified) for separate and disparate uses". This again goes to the heart of general concern over data aggregation.

Health data for private sector use

2013 will see an acceleration of moves to pass data without patient consent to public health and health research bodies. This is of particular concern in the light of increasingly sensitive genetic and epidemiological data that are available to practitioners and medical institutions.

---

[14] http://www.nytimes.com/2013/01/26/technology/eu-privacy-proposal-lays-bare-differences-with-us.html?_r=0

[15] http://online.wsj.com/article/SB10001424127887324478304578171623040640006.html#project%3DNCTCguideemail%26articleTabs%3Darticle

[16] http://technorati.com/technology/article/uk-government-plans-for-online-monitoring/

Website registration and verification

China has commenced a program to register all online bloggers[17] but this imposition is becoming increasingly attractive to governments across the world. ICANN has already taken the first steps to creating a verification system for website owners, and acceleration of this activity will spark substantial public concern over the coming year.

The Amber List

The Amber List comprises issues that were consistently raised by respondents, but which failed to achieve the top ten "Red List" of issues. These are:

Ambient intelligence and the "Internet of Things"

A number of respondents expressed concern over the development of a future generation Internet infrastructure that will soon comprise some 70 billion connected machines and - eventually - 70,000 billion smart physical and virtual "things" such as RFID devices. By 2020 there will be at least 50 billion smart connected devices, almost seven times the projected human population of the planet.[18]

Gerald Santucci of the European Commission explained why this issue is on the cusp of public concern:

> *The issue of course is not just the number, it is the upcoming reality that smart objects endowed with intelligence and unprecedented self configuring and self healing capabilities will make choices for us or on our behalf. It's not just more data that will be generated, it is new kinds of data, i.e. data sensed by humans' artifacts and processed by the IoT systems. In this new context, who will be the data subject? The data controller?*

Identity architectures

Governments across the world continue to build national infrastructures for identity, usually involving mandatory ID card and numbering systems for multiple uses. This trend follows aggressive selling of such systems, often by Western IT companies.

The system that is most likely to provoke controversy in 2013 is the Indian UID system. Indian IT commentator Vickram Crishna submitted that the system contained hidden and possibly sinister elements:

---

[17] http://techcrunch.com/2013/01/03/sina-weibo-accounts-of-prominent-bloggers-journalists-activists-shuttered-as-china-clamps-down-on-internet-users/
[18] http://www.futuristspeaker.com/2012/09/empowering-things-for-our-internet-of-things/

The Indian government's UID scheme enters its third year of enrollments, still far short of its goal, fortunately, covering mostly urban economically better placed people. The sole pilot, a rollout for distribution of subsidised bottled cooking gas, has failed. Despite this dismal showing, the government now mandates, possibly illegally, the use of 'voluntary' UID registration for a diverse bag of obligatory services. Its linkage with citizenship identification projects and national security may cloak a sinister purpose: relentless and purposeful surveillance.

Export of surveillance technologies to non-democratic regimes

The Arab Spring and other recent developments opened up the important issue of the relationship between Western tech developers and tyrannical governments that seek to exploit surveillance technology. Under the campaign leadership of organisations such as Privacy International[19] this exposure has led to the first stage of regulatory action by governments. It is anticipated that 2013 will further expose companies that engage in this practice.

The controversial brands of 2013

A significant number of respondents identified particular companies and governments that they believed would be most likely to spark controversy in 2013. These predictions mirrored media and political coverage over the previous year.

Google heads this list by a significant margin, followed by Facebook. This prediction is not surprising, given that these two players have taken the first and second “column inch” place in negative media coverage for at least the past three years. There was however a body of opinion that in view of Google’s involvement in a very wide spectrum of predicted controversies, it would attract an even greater proportion of negative coverage over the coming year.

[19] http://www.guardian.co.uk/world/2012/apr/07/surveillance-technology-repressive-regimes