AfriSIG 2014

Privacy Governance

Pria
.za
.africa

GLOBAL CONTEXT: Protect My Data

IT systems and business tools (enterprise data, (know your) customer data, profiling, analytics, relationship management, financial, health)

Records management policies (creation, retention and destruction of records, open data, open government)

Digital content ownership (eg. social media,) (users: personal data and intellectual property, rights and obligations)

Database ownership(source of data, use of data, rights and obligations)

Digital Content Ownership

- Should the subject of the digital content own the own digital content?

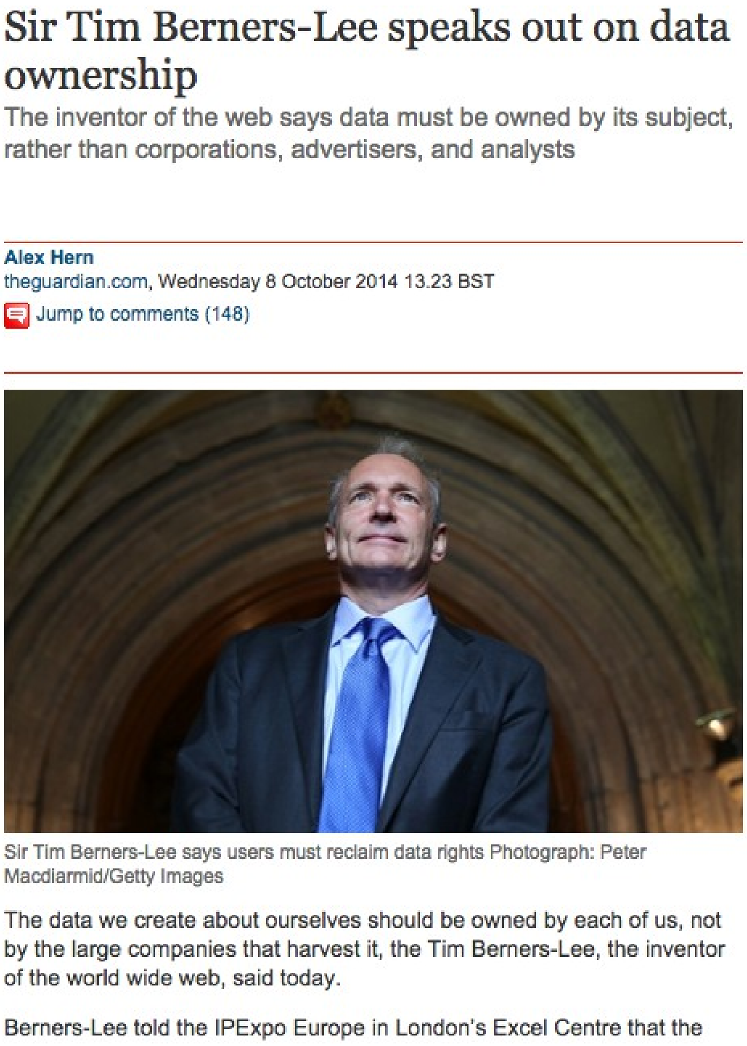
“What are these people going to do with that data? They’re going to target you with an ad which makes you feel a bit queasy. Targeted adverts are not the future.”

Sir Tim Berners-Lee

in The Guardian

“If you give [people] the ability to see how [data is] used and you ban its misuse then people are much more happy to open up to their data being used.”

Sir Tim Berners-Lee



Sir Tim Berners-Lee speaks out on data ownership

The inventor of the web says data must be owned by its subject, rather than corporations, advertisers, and analysts

Alex Hern
theguardian.com, Wednesday 8 October 2014 13.23 BST
Jump to comments (148)

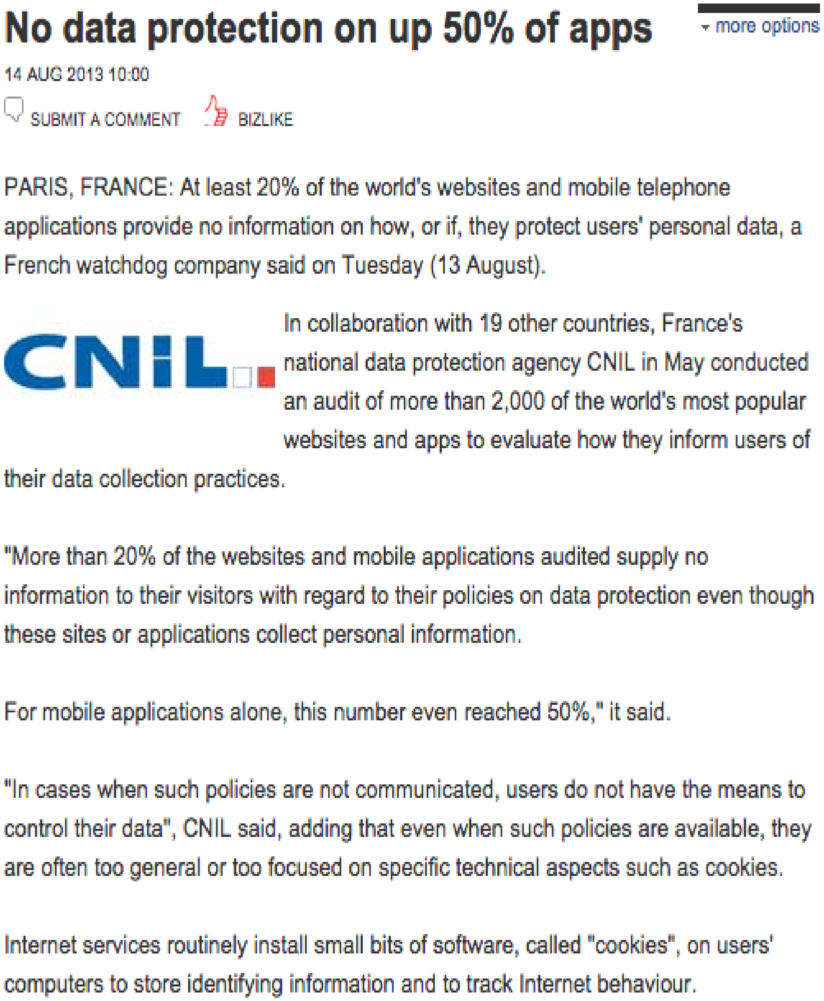
Sir Tim Berners-Lee says users must reclaim data rights Photograph: Peter Macdiarmid/Getty Images

The data we create about ourselves should be owned by each of us, not by the large companies that harvest it, the Tim Berners-Lee, the inventor of the world wide web, said today.

Berners-Lee told the IPExpo Europe in London's Excel Centre that the

App Ownership

- Data Protection for Apps
- Owners of App are responsible for protection of data collected
- Think of all of the information an App can collect about you
  - Health & sport monitoring apps
  - Medical apps
  - Messaging apps



No data protection on up 50% of apps

14 AUG 2013 10:00

PARIS, FRANCE: At least 20% of the world's websites and mobile telephone applications provide no information on how, or if, they protect users' personal data, a French watchdog company said on Tuesday (13 August).

In collaboration with 19 other countries, France's national data protection agency CNIL in May conducted an audit of more than 2,000 of the world's most popular websites and apps to evaluate how they inform users of their data collection practices.

"More than 20% of the websites and mobile applications audited supply no information to their visitors with regard to their policies on data protection even though these sites or applications collect personal information.

For mobile applications alone, this number even reached 50%," it said.

"In cases when such policies are not communicated, users do not have the means to control their data", CNIL said, adding that even when such policies are available, they are often too general or too focused on specific technical aspects such as cookies.

Internet services routinely install small bits of software, called "cookies", on users' computers to store identifying information and to track Internet behaviour.

Privacy in Africa: Are we asking Questions

SIM Card Registration in Africa

Does adequate technological and policy oversight exist to prevent SIM card registries from being misused?

What evidence is that that SIM card registries are actually contributing to crime reduction?

Are law enforcement agencies already using passive surveillance technologies like IMSI catchers?

Are passive surveillance technologies covered under existing legislation concerning the interception of communication?

https://manypossibilities.net/2012/09/35-reasons-to-worry-about-privacy-in-africa/

Encoding PRIVACY– REGULATORY Developments and Approaches IN AFRICA

WSIS Principles – Security and Privacy

- The WSIS Declaration of Principles state that **strengthening the trust framework, including information security and network security, authentication, privacy and consumer protection, is a prerequisite for the development of the Information Society** and for building confidence among users of ICTs. In order to achieve this, a global culture of cybersecurity needs to be actively promoted, developed and implemented in cooperation with all stakeholders and international expert bodies.

Clear association between information society intent and trust imperative

AU Convention

- Member States need to:
- Achieve a level of **technological security** adequate enough to prevent and effectively control technological and informational risks;
- Build an information society that respects **values,** protects **rights and freedoms,** and guarantees the security of the property of persons, organizations and nations;
- **Create a climate of confidence and trust**

African Declaration on Internet Rights and Freedoms

- ***Concerned*** at the continuing inequality in access and use of the Internet, and concerned at the increasing use of the Internet by state and non-state actors as a means of violating the individual’s rights to privacy and freedom of expression through mass surveillance and related activities;
- ***Recognizing*** the responsibility of States to respect, protect and fulfill human rights of all people, and the responsibility of Information and Communications Technology (ICT) companies and Internet intermediaries to respect the human rights of their users as consistent with the United Nations Guiding Principles on Business and Human Rights;

Privacy and Security

- **PRIVACY**
- Everyone has the right to privacy online including the right to control how their personal data is collected, used, disclosed, retained and disposed of. Everyone has the right to communicate anonymously on the Internet, and to use appropriate technology to ensure secure, private and anonymous communication.
- The right to privacy on the Internet should not be subject to any restrictions, except those which are provided by law, for a legitimate purpose and necessary and proportionate in a democratic society, as consistent with international human rights standards.
- **SECURITY ON THE INTERNET**

Personal Data Protection

- Personal data or information must only be collected and/or processed by States and non-State actors such as access providers, mail providers, hosts and other intermediaries, in compliance with well-established data protection principles, including: first, personal data or information must be processed fairly and lawfully; secondly, personal data or information must be obtained only for one or more specified and lawful purposes; thirdly, personal data or information must not be excessive in relation to the purpose or purposes for which they are processed; fourthly, personal data or information must be deleted when no longer necessary for the purposes for which they were collected.
- The collection, use, disclosure and retention of personal

Surveillance

- Mass or indiscriminate surveillance of the people and the monitoring of their communications constitutes a disproportionate interference, and thus a violation, of the right to privacy. Mass surveillance should be prohibited by law.
- The collection, interception and retention of communications data amounts to an interference with the right to privacy whether or not those data are subsequently examined or used.
- In order to meet the requirements of international human rights law, lawful surveillance of online communications must be governed by clear and transparent laws that, at a minimum, comply with the following basic principles: first,

Access to Information

- **RIGHT TO INFORMATION**
- Everyone has the right to access information on the Internet. The Internet must continue to facilitate the free flow of information.
- All information, including scientific and social research, produced with the support of public funds should be freely available to all

Right to Information and Open Data

- The internet offers new opportunities to access official information, and for governments to communicate with people, through the use of open data. Open data and new forms of online consultation can empower people to take a more active part in public affairs.
- Data and information held by government should be made publically accessible, including being released proactively and routinely, except where legitimate grounds for restricting access to such information exists in the relevant access to information legislation.
- Public and relevant private bodies have a duty to collect information on their operations and activities on behalf of their citizens. They also have an obligation to respect

APAI – African Platform for Access to Information Declaration, 2011

- Fundamental Right Accessible to Everyone. Access to information is a fundamental human right, in accordance with Article 9 of the African Charter on Human and Peoples' Rights. It is open to everyone, and no one should be privileged or prejudiced in the exercise of this right on account of belonging to a class or group howsoever defined, and whether in terms of gender, class, race, political association, occupation, sexual orientation, age, nationality, HIV status, and other bases as cited in many African constitutions. It is not required that anyone must demonstrate a specific legal or personal interest in the information requested or sought or otherwise required to provide justification for seeking access to the information.

  - http://www.africanplatform.org/fileadmin/user_upload/pdf/APAI-Declaration/APAI-Declaration-English.pdf

Privacy And AI in Africa: National Approaches

- Existence of the right to Privacy (Constitutional right?)
- Limitations on Rights
- Data Protection Principles in Law
- Right of Access to Information
- Procedures to fulfil right of access to information
- Regulatory Oversight over Privacy and Access to Information

AfriSIG 2014

- How will Africans contribute to global public policy setting and discourse?
- Lessons learnt in SA
  - In developing countries, issues of mobile uptake and mobile security and privacy are emphasised - mobile payments, spam, digital literacy
  - Accessibility of concepts of information privacy and access to information, cybercrime, e-signatures
  - End user confidence and trust in internet banking in developing countries
  - Confidence and trust in e-government services
  - Institutional effectiveness lessons learnt – resourcing, skills,
  - [illegible]

Pria Chetty

- Pria.chetty@endcoc
    - endcode.org

THANKS, QUESTIONS?

ENDCODE

Tech. Law. Policy. Africa.

References

- http://ico.org.uk/for_organisations/data_protection/security_measures)

- http://www.theguardian.com/money/2012/sep/03/do-you-own-your-digital-content

- http://www.theguardian.com/technology/2014/oct/08/sir-tim-berners-lee-speaks-out-on-data-ow
  ema_827

- http://www.bizcommunity.com/Article/75/542/98352.html

- http://ico.org.uk/Youth