



A review of user online privacy capabilities

Anna Magnisali, Nikolaos Tsalis, Vasileios Stavrou

{p3080229, ntsalis, stavrou}@aueb.gr

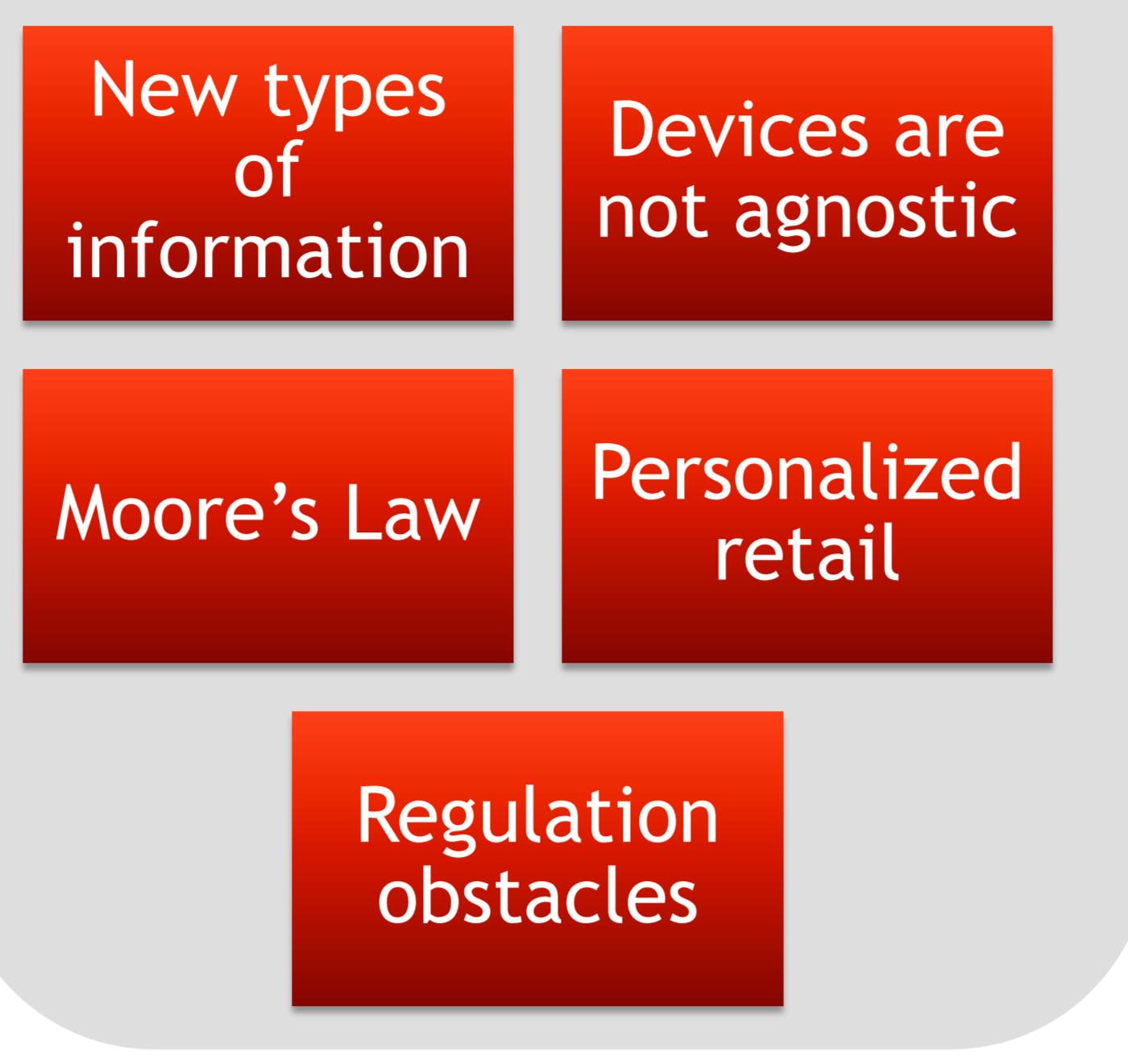
Information Security & Critical Infrastructure Protection (INFOSEC) Laboratory
Dept. of Informatics, Athens University of Economics & Business (AUEB), Greece



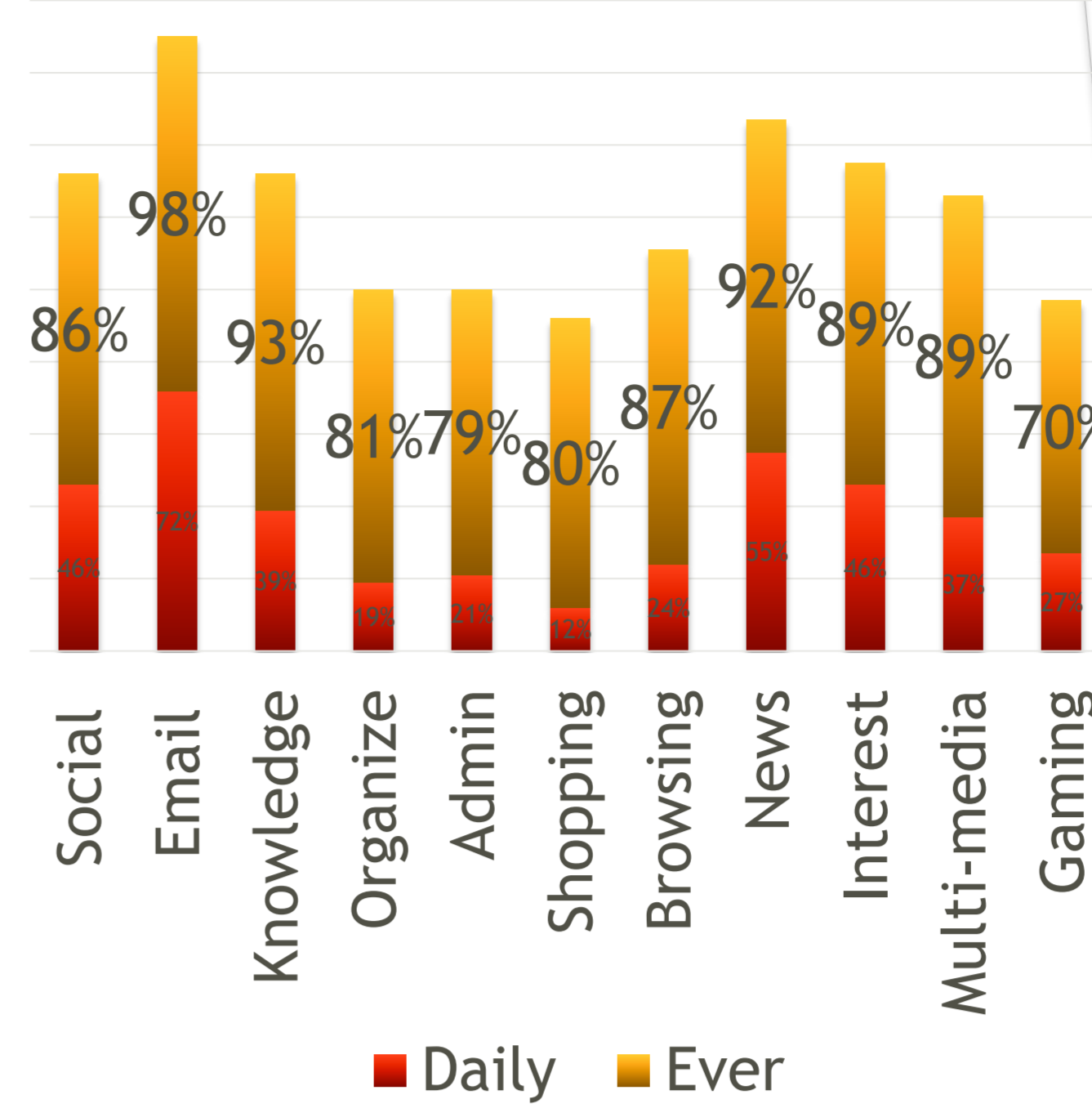
Major data breaches

NO. OF RECORDS STOLEN	RECORDS (MILLION)	YEAR IT STARTED
ATHEM	80	2015
HOME DEPOT	50	2014
JP MORGAN CASE	76	2014
TARGET	70	2014
EBAY	145	2013
LIVING SOCIAL	50	2013
ADOBE	36	2013
EVERNOTE	50	2012
MASSIVE AMERICAN BUSINESS HACK	160	2011
ZAPPOS	24	2011
TIANYA	28	2010
STEAM	35	2009
SONY PSN	77	2009
ROCK YOU	32	2008
HEARLAND	130	2007
US MILIATRY	76	2007
TK / TJ MAX	94	2006
AOL	20	2006
DEUTSCHE TELECOM	17	2005
AOL	92	2005

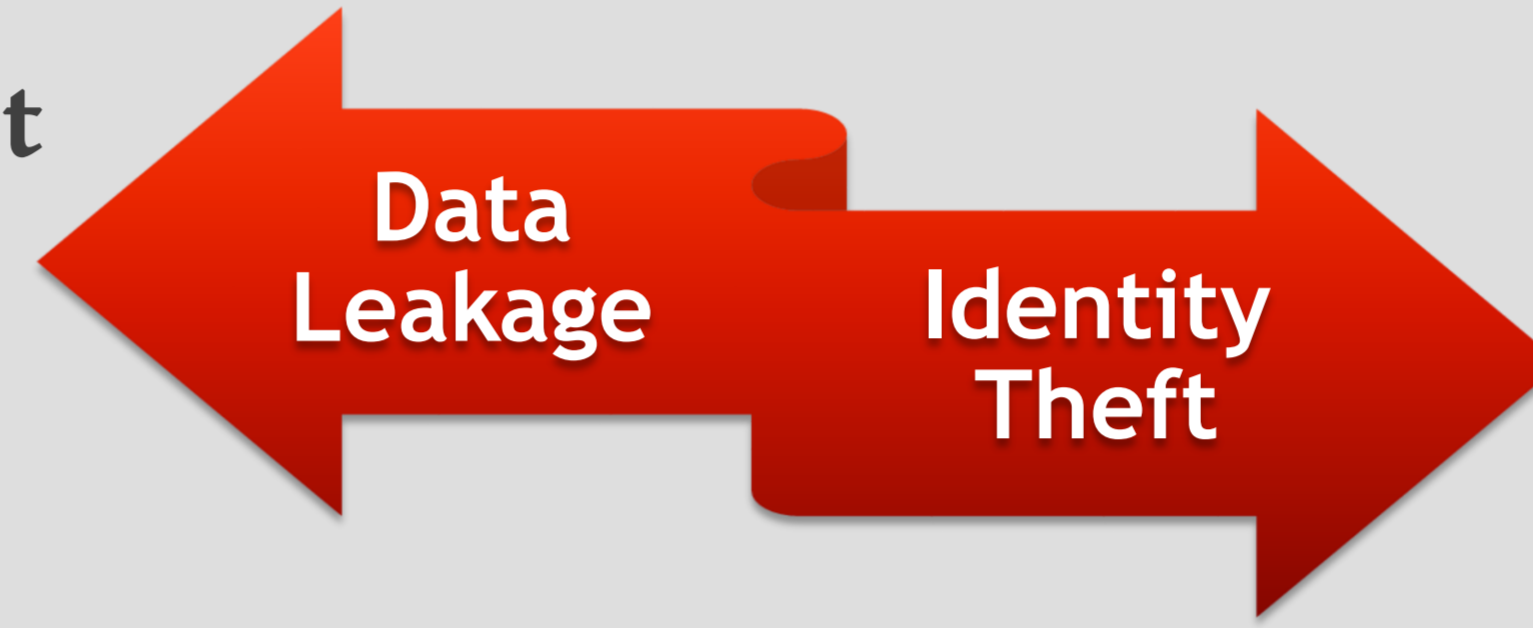
Web 2.0 vs. Privacy



Online Behavior



Which are the most dangerous online privacy threats?



User privacy perception and awareness



How do privacy threats affect CIA and human rights?



Threat hierarchy/categorization

Level 1	Information / Data Leakage	Social Engineering	Identity Theft	Personalization
Level 2	Cyber Bullying, Reputational Attacks, Sensitive Data Exposure, Backup Data Exposure, Intellectual Property Theft	Pretexting, Phishing, Baiting, Tailgating, Dumpster Diving	Unauthorized Use of Name, Shoulder surfing, Criminal Financial Gains	Data storage, Unauthorized Identification, Physical Damage (location based)
Level 3	Hacking (authentication based attacks, cracking, key-logging malware, phishing attacks), backdoors, SQL injection, buffer overflow exploits, brute force attacks, rootkit, tampering, privilege abuse, foot-printing, admin-ware, scan networks, disable controls, POS intrusions, Card Skimmers, Cyber - espionage, DoS attacks	Social engineering attacks, fast track pentesting, third party modules, metasploit framework, SET configuration), Phishing, fishing Scams	key loggers (Trojan Horses), email phishing, drive-by downloads, code injections, botnets, cross-site scripting	cookies, tracking pixels, all sorts of online data (mouse overs, clicks, impressions, play/stop button counters etc.)

A centralized (left) vs. a decentralized online social network (OSN)



Countermeasures

Level 1	Info/Data leakage	Social Engineering	Identity theft	Personalization
Level 2	Educate individuals & organizations, risk assessment/critical data analysis, retain best practices in backing up, trademark registration	Educate employees & individuals, retain best practices in physical penetration testing,	Educate individuals & organizations, retain best practices in creating passwords	Educate individuals & organizations, utilization of privacy-enhancing tools

No. of Facebook privacy policy revisions

Year	Revision Date	Number of Revisions
2005	28-Jun-05	1
2006	22-May-06	3
	05-Sep-06	
	23-Oct-06	
2007	12-Sep-07	2
	06-Dec-07	
2008	26-Nov-08	1
2009	09-Dec-09	1
2010	22-Apr-10	3
	05-Oct-10	
	22-Dec-10	
2011	07-Sep-11	2
	23-Sep-11	
2012	08-Jun-12	2
	11-Dec-12	
2013	15-Nov-13	1
2014	--	0
2015	30-Jan-15	1

References

- Gritzalis D., Stavrou V., Kandias M., Stergiopoulos G., "Insider Threat: Enhancing BPM through Social Media", in Proc. of the 6th IFIP International Conference on New Technologies, Mobility and Security, IEEE Press, 2014.
- Gritzalis D., Kandias M., Stavrou V., Mitrou L., "History of Information: The case of Privacy and Security in Social Media", in Proc. of the History of Information Conference, Law Library Publications, 2014.
- Gritzalis D., "Insider threat prevention through Open Source Intelligence based on Online Social Networks", Keynote address, 13th European Conference on Cyber Warfare and Security (ECCWS-2014), Greece, 2014.
- Kandias M., Mylonas A., Virvilis N., Theoharidou M., Gritzalis D., "An Insider Threat Prediction Model", in Proc. of the 7th International Conference on Trust, Privacy and Security in Digital Business, pp. 26-37, Springer (LNCS 6264), Spain, 2010.
- Kandias M., Galbogini K., Mitrou L., Gritzalis D., "Insiders trapped in the mirror reveal themselves in social media", in Proc. of the 7th International Conference on Network and System Security, pp. 220-235, Springer, 2013.
- Kandias M., Mitrou L., Stavrou V., Gritzalis D., "Which side are you on? A new Panopticon vs. privacy", in Proc. of the 10th International Conference on Security and Cryptography, pp. 98-110, ScitecPress, 2013.
- Kandias M., Stavrou V., Bozovic N., Mitrou L., Gritzalis D., "Can we trust this user? Predicting insider's attitude via YouTube usage profiling", in Proc. of 10th IEEE International Conference on Autonomic and Trusted Computing, pp. 347-354, IEEE Press, 2013.
- Kandias M., Virvilis N., Gritzalis D., "The Insider threat in Cloud Computing", in Proc. of the 6th International Conference on Critical Infrastructure Security, pp. 93-103, Springer, 2013.
- Kandias M., Stavrou V., Bozovic N., Gritzalis D., "Proactive insider threat detection through social media: The YouTube case", in Proc. of the 12th Workshop on Privacy in the Electronic Society, pp. 261-266, ACM, Germany, 2013.
- Kandias M., Mitrou L., Stavrou V., Gritzalis D., "YouTube user and usage profiling: Stories of political horror and security success", in e-Business and Telecommunications, Springer, 2014.
- Kotzanikolaou P., Theoharidou M., Gritzalis D., "Cascading effects of common-cause failures on Critical Infrastructures", in Proc. of the 7th IFIP International Conference on Critical Infrastructure Protection, pp. 171-182, Springer, USA, 2013.
- Mitrou L., Kandias M., Stavrou V., Gritzalis D., "Social media profiling: A Panopticon or Omnipoint tool?", in Proc. of the 6th Conference of the Surveillance Studies Network, Spain, 2014.
- Pipyras K., Mitrou L., Gritzalis D., Apostolopoulos T., "A cyber attack evaluation methodology", in Proc. of the 13th European Conference on Cyber Warfare and Security, Athens, 2014.
- Theoharidou M., Kotzanikolaou P., Gritzalis D., "Risk-based criticality analysis", in Proc. of the 3rd IFIP International Conference on Critical Infrastructure Protection, Springer, USA, 2009.
- Theoharidou M., Tsalis N., Gritzalis D., "In Cloud we Trust: Risk-Assessment-as-a-Service", in Proc. of the 7th IFIP International Conference on Trust Management, pp. 100-110, Springer (AICT 401), Spain, 2013.
- Tsalis N., Theoharidou M., Gritzalis D., "Return on security investment for Cloud platforms", in Proc. of the Economics of Security in the Cloud Workshop, pp.132-137, IEEE Press, United Kingdom, 2013.
- Tsalis N., Virvilis N., Mylonas A., Apostolopoulos A., Gritzalis D., "Browser Blacklists: A utopia of phishing protection", in Security and Cryptography, M. Obaidad (Ed.), Springer, 2015 (to appear)
- Virvilis N., Tsalis N., Mylonas A., Gritzalis D., "Mobile devices: A phisher's paradise", in Proc. of the 11th International Conference on Security and Cryptography, pp. 79-87, ScitecPress, Austria, 2014.
- Virvilis N., Mylonas A., Tsalis N., Gritzalis D., "Security Busters: Web Browser security vs. rogue sites", Computers & Security, 2015 (to appear)