

## 2012 Data Privacy Roadmap

Data Privacy Day gives us an opportunity to reflect on the past year and set our focus on the new year. A quick look back shows 2011 as a tumultuous year for personal data privacy. Tens-of-millions of consumers were impacted by corporate, government, and medical data breaches. We saw the highest volumes of malware and cybercrime in history. But we also saw some gains. Global spam volumes dropped, and data privacy is now being discussed broadly within governments, companies, in public forums and in homes. We've seen regulatory agencies increase their monitoring and mete out punishments against offending groups and companies.

We need to take a moment and applaud the dedication many organizations have shown towards improving consumers' data privacy. These include security companies, large platform developers, many individual service providers, non-profit groups, and others. We need to encourage them to continue this work finding ever more collaborative ways to leverage the work that has been done and push into new areas of safety.

### **We're at a historic crossroads in the history of technology and personal data privacy.**

Heavy regulation that stifles the autonomy, speed and creativity of internet development will not serve us well; neither will an environment where a handful of companies can ignore established privacy, safety and security norms for their own profit. Society is not served when companies rush to deploy de facto standards before consumers—or —our representative bodies, our governments—can review and set privacy, safety, and security boundaries. Before creating technological solutions, let's ask if there are ethical, privacy, safety, or security issues that should first be defined.

Oversight helps us collectively grapple with the ethical questions of 'shoulds and should-nots' so that the entire focus is not just with the 'can and cannots'. There is humility in a reflective evaluation process that is largely lacking in our current market-driven, no holds barred, users' information is the currency so grab it, rush-forward internet world.

We need clarity about the security and data privacy requirements that should be a prerequisite in internet products and services for consumers; — this must happen before products are developed, not after tremendous damage has been done.

Given the severity of data breaches in 2011, a stronger set of standards must be enforced this year among companies storing consumer data. We simply cannot tolerate that sensitive information is stored unencrypted, or that information protection is an afterthought. As Commerce Secretary Gary Locke candidly [put it](#) a year ago, "The internet will not reach its full potential until users and consumers feel more secure and confident than they do today when they go online."

This year will also require additional focus on cybercrimes. Predictions anticipate an expansion of existing forms of malware and expanding and emerging new threats, particularly around mobile banking and e-commerce, cloud computing and social engineering exploits.

### **2012 resolutions for Data Privacy:**

#### ***Consumers:***

- Install *effective* security software on every internet connected device—including smartphones—and set these to automatically update. At the end of last year, Commtouch reported that an average of 209,000 unprotected computers were being taken over by criminals for use in botnets *every single day*. In addition to stealing your data, churning out spam, scams, and malware, these botnets are wielded by criminals and can create havoc on companies and governments, military units—even the power grid. Failure to protect your devices not only exposes you to risk, it places society in harm's way.
- Stop clicking on unknown links! Spam, scams and phishing exploits aren't going away. Whenever you click on a link in an email, a social networking site, or a link on another web page etc., you are gambling that it will take you to the safe site you intended to visit. Stop gambling. Take 30 seconds to find the site yourself and avoid the potential malware that will mess up your machine, steal your information, and expose your contacts to risk. Your devices and your privacy are worth the time.

### **Companies:**

- Inform users about their online experience *in advance* of any potential safety or privacy risks in products, web programs and services such as instant messaging programs, social networking sites, location technology, or with Internet enabled devices like cell phones, game consoles etc. This will help users make safety and privacy choices that are appropriate to their circumstances.
- Provide complete, easily understood information about every safety and privacy feature in a product or service. Offer age appropriate recommendations by feature, and make them easy to find and understand.
- When services are upgraded, inform users of new features or changes to existing features and their impact on their safety or privacy *in advance* of the rollout. Additionally, users should have a clear way to opt out of, or block, any features they're uncomfortable with.
- Provide users with the privacy and safety policies of your online products and services.
  - These should be easy to find and written in terms that are easy to understand.
  - The terms of any third-party applications should be explicitly displayed as part of the transition process between services, so that users always understand the terms and conditions under which they are protected—or exposed. If there are privacy and safety choices offered by the third party application, customizing your settings should also be a part of the transition.
- Provide users *advanced notice* of any intended changes in the terms and conditions that will affect their safety, privacy, or alter the terms in any other substantial way. This notice may come in the form of an email, text, or during your next login experience.
- Take steps to bring your data privacy practices and policies up to an industry standard of excellence.

### **Countries:**

- Ensure that internet services are built with proper safety, security and privacy impact evaluations by creating clear regulations. Tightly monitor products that impact consumers' daily lives, making sure that these products are in compliance with baseline safety features.
- Provide public service messages with useful, actionable information. Failure to do so results in a high percentage of the population remaining unaware of the safeguards they need to have in place to be safer online.
- Fund internet safety education/media literacy/data privacy programs in schools. A study released last May found cyber education far from where it needs to be<sup>i</sup>. Among the findings, were that 36 percent of teachers received zero hours of professional development related to online safety, security and ethics in the past year. All told, 86 percent received less than six hours of related training. Failure to train teachers and educate students is a failure to prepare future generations to compete in a global market.
- Enhance law enforcement's digital forensics capabilities. In an era of rapidly expanding internet crimes, we are not doing enough to train and deploy officers with internet specialties, and those few we have don't receive the technical resources they need. There is an appalling shortage of cyber-crime labs; officers are often struggling against antiquated technologies and old state and federal laws that make bringing criminals to justice difficult.
- Protect consumer data. For most consumers, information posted and exposed by the federal, state, county and local government agencies represents their greatest risk of becoming a victim of identity theft. Although some "right-to-know" laws are necessary, these need to focus on government actions and stop at the door of private individuals.

### **Conclusion:**

Together we hold the keys to the internet of the future. The actions we take this year will not only impact our personal privacy, but the privacy of generations to come. Please join us in investing efforts into creating a safe, respectful and secure internet environment. By next year, iKeepSafe hopes we'll be able to look at an in-depth status report that will demonstrate that we've not only held ground, but strengthened our position.

For additional information:

Jennifer Finlinson

iKeepSafe

[Jennifer@iKeepSafe.org](mailto:Jennifer@iKeepSafe.org)

(801) 623-3009

---

<sup>i</sup> 2011 State of Cyberethics, Cybersafety and Cybersecurity Curriculum in the U.S. Survey, <http://www.microsoft.com/presspass/press/2011/may11/05-04msk12digitalpr.msp>