



Christopher Boam

*Counsel for Internet & Global Ecommerce
MCI, Inc., International Affairs*

on behalf of ***WITSA***

The World Information Technology and Services Alliance



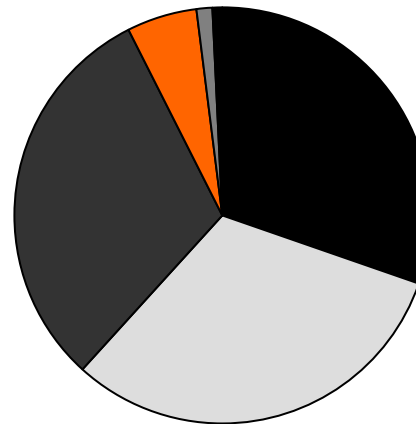
Users on the Internet – Sept 2002

- **CAN/US - 182.67M**
- **Europe - 190.92M**
- **Asia/Pac - 187.24M**
- **Latin Am* - 33.35M**
- **Africa - 6.31M**
- **Mid-east - 5.12M**

• **Total - 605.6 M**

* *Includes Central and South America*

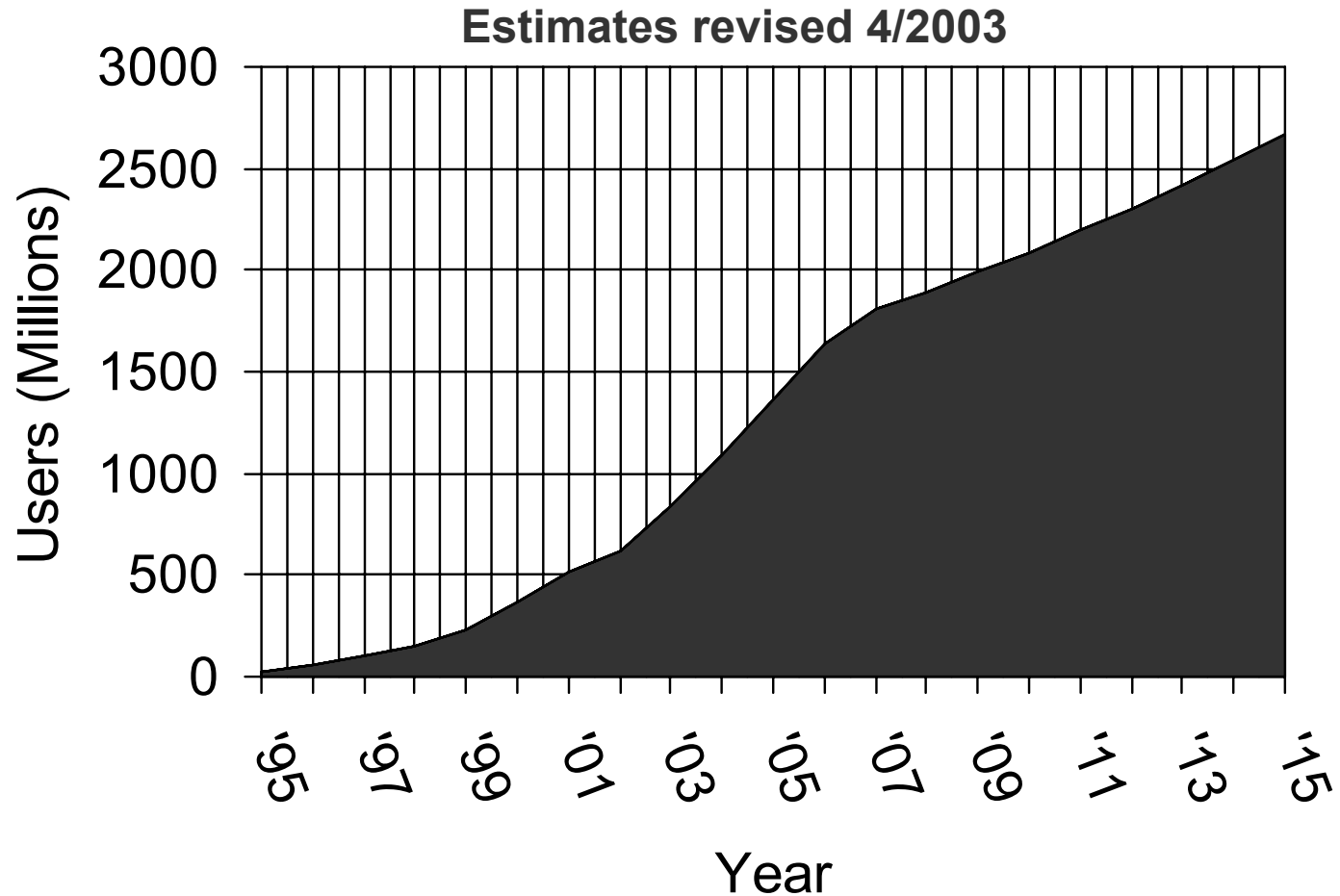
(Source: www.nua.ie)



- **CAN/US**
- **Europe**
- **Asia/Pac**
- **Latin Am**
- **Africa**
- **Mid East**



Internet User Trends



(Source: Nua Internet Surveys + V.Cerf projections)



Data Preservation vs. Data Retention

- Mandatory data retention requirements (for service providers to “pool” network data for law enforcement investigative purposes) pose significant risks by:
 - requiring companies to create enormous data pools – potential targets for misuse;
 - requiring security measures at significant cost; and
 - ignoring technical infeasibility to effectively search retained data.
- The issue of whether to impose mandatory data retention should be addressed in a manner that reflects:
 - the limited context in which retained data would be useful to law enforcement;
 - the enormous risks and possible costs to service providers; and
 - the successful implementation of more efficient and effective investigative tools such as data preservation.



Content Liability and “Blocking”

- Legislation and regional codes of practice often fail to embody three key components with regard to the liability of a hosting (or non-hosting) service provider:
 - First, there must be recognition of the fact that a service provider that does not host the alleged illicit content has little if any effective technical ability to block it. And forcing an ISP to attempt a block can often exacerbate the problem.
 - When a service provider does host material found to be illicit, there needs to be a process by which *law enforcement* makes the determination as to what is “illegal,” etc., based upon a legal or regulatory scheme that defines such material.
 - And finally, there must be formal adherence to process by law enforcement in requiring ISPs to “takedown” designated material in order to limit liability for acting in accordance with the order.



Council of Europe Declaration

- “Freedom of Communication on the Internet” (May 2003) urges member states:
 - 1. To refrain from subjecting online content to tougher restrictions than those imposed on other means of content delivery.
 - 2. To encourage self- or co-regulation of Internet content.
 - 3. Not to block or filter content or deny public access to it, with the exception of filters aimed at protecting children.
 - 4. To encourage universal access to Internet communications and information services on a nondiscriminatory basis at reasonable cost.
 - 5. Not to subject the provision of online services to special authorization schemes solely on the ground of the means of transmission used.
 - 6. Not to hold ISPs liable for Internet content when they merely transmitted information or provided access. However, the CoE said, ISPs could be held co-responsible if they didn't take down sites when they became aware of their illegal nature.
 - 7. To respect the decision of users to remain anonymous online.



(Located at: http://www.coe.int/T/E/Communication%5Fand%5FResearch/Press/News/2003/20030528_declaration.asp)



Data Protection and Privacy

- Development of new or improved DP standards and legislation should focus on four key imperatives:
 - **Relevant Risks** – Create rules that focus on the risk attributable to misuse of certain types of data in setting the level of protection for that data;
 - **Consistent Implementation** – Ensure that national legislation cannot embellish regional framework or other international DP requirements with added protections that frustrate the possibility of cross-border compliance;
 - **Flexible Compliance Options** – Enable regulatory authorities to review and give the “stamp of approval” to appropriate industry and NGO-developed compliance contracts, codes and procedures; and
 - **Consultation** – Industry understands that its role in DP compliance supports its mission to achieve and retain customers, and thus, industry consultation at all levels of DP legislative development will improve compliance and enforcement.



Privacy “Self Help”

- **Ask questions** – Before you give a Web site your email address, phone number, home address, check out their privacy policy or email them a question. If you don't get a good answer, move on.
- **Protect yourself from Harvesters** – People that want to send you Spam will look for your email address anywhere and everywhere. Consider creating a “disposable” email address to use in public postings, online purchases and online chatting.
- **When it comes to Spam, don't talk to strangers** – Which means, if you get Spam, and you've never heard of the company or sender, don't waste your time sending them an email to take you off their list. Unfortunately, 9 times out of 10, they're simply hoping you respond so that they can see your address is “live” and send you more Spam.
- **Never ever use a social security or government ID number online** – Most reputable online companies both in the US and abroad will never ask you for it, and if they do, they'll give you several other options for you to identify yourself. You don't want that number misused, online or anywhere else, so don't use it – period. If somebody online says you need to use it, then take your business elsewhere.





Christopher Boam

*Counsel for Internet & Global Ecommerce
MCI, Inc., International Affairs*

on behalf of ***WITSA***

***The World Information Technology
and Services Alliance***

