

Caution: Please Do Not Cite Without Explicit Written Authorisation From The Author. This is one chapter of a manuscript being edited for the book: *Ordering Chaos: Regulating the Internet*. Copyright has been assigned to the publisher, Thomson Learning.

Framework For Regulating The Internet

Introduction

One of the questions policy-makers ask about regulations concerning the internet is: where do we begin? This chapter aims to answer that question. It looks at various modes of regulation and then draws up a framework for regulation in the internet arena. Here regulation refers not only to black-letter laws but also to the entire regulatory mechanism from the formulation of rules to the monitoring and enforcement of compliance. Ultimately, rules must be backed up with effective sanctions to punish offenders and, ideally, also to reward the compliant. The elements of sanction and reward are important because without them it is impossible to distinguish law-abiders from law-breakers and eventually regulation fails.

It is often assumed that because the internet is such a personal medium, it is impossible to use law against it. The thoughts flow along these lines: how can the authorities pin me down if I can be anonymous, if I cannot be traced and if what I do cannot be stopped. Such thinking is actually not very far from traffic offences such as speeding or illegal parking. No county in the world can enforce its speeding or parking laws with 100 percent efficacy. The car is a personal transport medium. Perhaps the biggest difference with the internet is that cars have a physical presence that make them more noticeable. Still, the point is that no police force enforces the speeding laws with 100 percent efficacy.

Law enforcement does not work so much through punishing offenders although that is certainly important but through preventing the offence from happening. That is, they work less through punishment than through the threat of punishment. Does it work on the internet? The evidence suggests it does. When the US Naval Academy punished 85 trainees for downloading copyrighted movies, music and computer software, the volume of downloads shrank dramatically.¹ The key, however, is that there must be some element of sanctions, which of course can be done by the Naval Academy. As this chapter will show, it is possible to apply the law to the internet, albeit with more limited results.

Lawrence Lessig suggests that there are four modalities of regulation that could be applied to the internet:

- markets (by price and availability).
- social norms (by expectation, encouragement, or embarrassment), and
- architecture (what the technology permits, favours, dissuades, or prohibits),
- laws (by government and private sanctions and force).²

These are broad modes. For example, as a mode law encompasses self-regulation. These modes are not mutually exclusive and in fact can and do overlap. A combination of modes may be necessary to address a problem. Spam and privacy concerns are two classic examples. A mix of social norms, technology and laws would be needed to ensure that the concerns are met.

¹ Nelson Hernandez and Amy Argetsinger. 2003. Midshipmen Disciplined Over Downloads. Washington Post. April 16. B3. <http://www.washingtonpost.com/wp-dyn/articles/A34564-2003Apr15.html>. (29 December 2003).

² Lawrence Lessig. 1999. Codes

With the internet, there is an additional level of complexity—international cooperation would be needed as well. For example, Australia, one of the countries at the forefront of regulating the internet, is looking at a mobilizing international support for spam.³

Modes of Regulation

Market Mechanism

By market mechanism is meant the use of market forces as a regulatory or disciplinary device. If the terms and conditions of the merchant one is dealing with are not favorable, one shops around to find a more favourable merchant. The market mechanism works in many, but not all situations. For example, using such a mode assumes informed consumers in a competitive market. Where these conditions are not met, there is market failure.

Arguably, there is no pure market-mechanism regulatory regime in the world. At the very least, one needs a contract to seal a deal and contracts are agreements enforced by the courts. So what is meant is the predominant reliance of market discipline in this mode. The market can be a disciplining force if a firm that violates the rules, say of fairness, is exposed to other buyers. The fear of reputational loss leading to monetary loss keeps the seller in check.

Because such a check requires the dissemination of information to the market, self-regulatory codes can be used in a market mechanism where there is informational asymmetry—a state that exists where one party, typically the seller, has more information than the other. The seller gives some additional information about its goods and services and thereby hopes to differentiate itself from the rest of the field. It is then up to the consumer to decide if the additional information is important enough to sway the decision.

An example of the market mechanism at work is Platform for Privacy Preferences (P3P). Although it could also be categorised as an example of “regulation through technology”, this technical standard treats privacy as a negotiable commodity instead of a human right. Websites that use P3P inform visitors of their privacy policies and it is then up to the visitor to accept or reject.

There are several advantages to using the market mechanism. First, there is the low cost of regulation because it is the market that takes care of regulating and of compliance. Second, the market mechanism allows companies and consumers maximum freedom of choice and action. Third, the market mechanism is dynamic in allowing rules to change to suit preferences over time.

The disadvantages are that first it does not protect the individual consumer. That is, it protects consumers as a group because that group can stand up to the seller. But as an individual, the consumer is in a much weaker bargaining position. Second, the market mechanism does not work when there is market failure. This can be a definitional problem in that the same set of facts may be interpreted to mean market failure by some and otherwise by others.

Social Norms

A norm that is widely accepted on the internet is that posts to Usenet groups should be on topic, that is, relevant to the group. As the husband and wife team of lawyers, Canter and Siegel, learnt when they advertised their immigration services on more than a thousand Usenet groups, the internet community can punish egregious breach of that norm. The more traditional methods included sending pizzas and magazine subscriptions to the office. Others sent the Bible (because of the size and the contents) to the mailbox. More high-tech efforts included the development of a

³ Declan McCullagh. 2003. Australia mulls global antispam effort. CNET News.com. April 16. <http://zdnet.com.com/2100-1105-997131.html> (29 December 2003).

software program to seek out and remove the Canter and Siegel posts from the Usenet. In the end, various ISPs terminated their accounts.⁴

Sysadmins have also banded together to apply the “death penalty” to ISPs whom they feel have not done enough to combat Usenet or email spam. In both instances, the death penalty consists of denying service.⁵

Technology

The nature of the internet is such that technology is always considered as one of the options to be explored in solving problems. Of course, not every problem can be solved through the use of technology but some can.

An early use of technology was the deployment of cancelbots to remove unwanted postings on Usenet groups. The use of cancelbots, however, must necessarily be limited because there are few widely-accepted norms on the internet in the first case.

However, organisations may have their own norms and here, technology can be more easily deployed. The University of Florida developed a program that warns students against peer-to-peer file sharing while it scans their computers. If the program detects file sharing, it cuts off network access for 30 minutes and issues a warning to the computer. A second offence results in network access being denied for five days; a third offence leads to indefinite suspension of network access and sends the case to the university’s disciplinary process. University officials report a dramatic drop to peer-to-peer file sharing.⁶ The University of Nevada, Reno, credits its success in avoiding copyright problems to its close monitoring of network traffic.⁷ In the US, an increasing number of ISPs are scanning email attachments to reduce the spread of viruses.⁸

In the area of online privacy, there have been a number of creative proposals, although each seems to face the limitation of not being able to address the problem sufficiently. For example, some software, such as Zero-Knowledge before the company went defunct, disguise the user. In effect, this bypasses the privacy issue because the merchant still collects information about the end-user but a “made-up” end-user. This approach is not satisfactory because the business would not have information about the consumer. The costs of acquiring and serving customers increase and these costs will eventually be passed back to the consumer.

Another creative use of privacy technology, P3P, faces the problem of not being able to protect privacy sufficiently without offline laws in the first case. A website owner is supposed to rate the site on a privacy scale. A visitor would set his or her privacy preference at a certain level. If the website visited has a lower privacy threshold, the user is alerted. He or she is then given sight of the policy and can then decide whether to visit or transact on the site. In P3P, the website owner holds out a standard of privacy on the site; if the site owner breaches the standard promised, the website visitor has no immediate recourse. A supporter of P3P, the Center for Democracy and

⁴ Charles Arthur. (1994). A Spammer in the Networks. *New Scientist*. Vol. 144. Available at <http://www.kkc.net/cs/new-sci1.txt> accessed September 2004.

⁵ Check: In other instances, the self-appointed SubGenius Police Usenet Tactical Unit Mobile (S.P.U.T.U.M.), in collaboration with system administrators, has exacted the “Usenet death penalty” on service providers that allow their customers to post unsolicited bulk advertisements (known as “spam”).

The death penalty bars all messages from any subscriber of the recalcitrant service provider. Similarly, the managers of the “Realtime Blackhole List” and other anti-spam activists identify Internet service providers who, in the activists’ opinion, have not done enough to prevent spammers from using their email relay systems to send spam email to third parties.

⁶ Automated Tool Enforces Student P2P Restrictions. *Wired News*, 3 October 2003. <http://www.wired.com/news/digiwood/0,1412,60613,00.html> (29 December 2003).

⁷ Network Monitoring At UNR. 2003. *Reno Gazette Journal*, 13 September. <http://www.rgj.com/news/stories/html/2003/09/13/51606.php> (29 December 2003).

⁸ ISPs Plan To Scan All E-Mail Attachments. 2003. *Washington Post*, 27 August <http://www.washingtonpost.com/wp-dyn/articles/A54406-2003Aug27.html>.

Technology, has said that “P3P cannot protect the privacy of users in jurisdictions with insufficient data privacy laws” and “cannot ensure that companies follow privacy policies” (Mulligan, 2000). What P3P hopes to achieve is accountability through transparency. The technology makes it easier to locate and compare privacy policies. It is then up to the consumer to decide to transact based on understanding the policy.

In 2001, a Dutch-led consortium announced that they had been awarded a three-year 3.2 million Euro (about US\$3 million then) contract from the European Community and Netherlands’ Ministry of Economic Affairs to create a Privacy Incorporated Software Agent (PISA) that would meet the requirements of the European Union data protection directives. PISA plans to develop a privacy enhancing technology (PET) architecture by 2002 and to develop a test version of the program by 2004.⁹

Experience suggests that PISA, in common with such technologies, would more likely play a role supplementary to the law.¹⁰ But as the EU has a data protection law, PISA would enter an environment in which it may have a chance to succeed.

Government Legislation

The most commonly understood mode of regulation is government legislation, which is essentially the use of decree. Its advantage is certainty—clear rules and certain enforcement. Such certainty is not to be lightly dismissed because the lack of certainty hampers business activity, which hinders the growth of the industry.

But there are major drawbacks in applying government legislation to the internet. The most significant is that the Net is still in its developmental stage. Laws, however, tend to be rigid and slow to change and in fact they need to be so, for certainty. Locking in laws that regulate an industry in its nascent stage will hinder the development of the industry. Second, there is the cost of compliance. Depending on what is required, the costs can be high. The US’s Children’s Online Privacy Protection Act, which came into effect in April 2000, has forced some sites to close those sections that cater to children because of compliance costs.¹¹

As will be argued in this book, which mode of regulation to use depends to a great extent on the context to which the regulation is intended to apply. For example, some modes are better suited than others depending on what is being regulated. In offline advertising for example, a combination of industry self-regulation and government legislation applies; there is no reason to think that in the online world, there should be a wholly different approach. In other cases, the law has been shaped through iteration, with first movers suffering the disadvantage of being pioneers. Thus laws that exempt network providers from liability for content they merely carry have evolved. Chapter 7 traces the evolution and highlights the need for industry inputs for internet regulations. In yet other cases, the mode will depend on the severity of the problem. Thus spam has grown to such proportions globally that there is an outcry for government legislation, as opposed to industry self-regulation.

In short, there is no one mode for regulation. Self-regulation, much touted as the preferred mode of regulation for the internet, has its limitations. The trick is to be open to the mode that best suits the situation on hand. If this sounds like the contingent theory of regulation, it is because the regulations are still at an experimental stage. Regulators are still learning how to regulate the internet and academics are still arguing over both the rules and the mode.

⁹ TNO-FEL. 2001. Fast and Safe Internet Work with PISA, January 17.

http://www.tno.nl/instit/fel/pisa/press_release_start_pisa_17012001.html (accessed January 31, 2001).

¹⁰ Burket, H. (1997). Privacy-enhancing technologies: Typology, critique, vision. In P. Agre & M. Rotenberg (Eds.), *Technology and Privacy: The New Landscape*, 125-142. Cambridge, MA: MIT Press.

¹¹ Net privacy law costs children’s sites. *USA Today*, 2000, September 14.

<http://www.usatoday.com/life/cyber/tech/cti526.htm> (accessed January 31, 2001).

The following framework should therefore be seen that light: it is an attempt to put into a structure that which is hotly debated. The following framework was developed some years back with my colleague, Yeo Tiong Min, and has proven to be robust, at least to debates. One source of comfort is that the Internet Act in the US state of Virginia, encompasses the entire framework save for one key area—copyright. And the reason for that is that US federal law applies to that area.

Framework

The following framework for regulating the internet is premised on the observation that in many countries, the issue is not whether the internet should be free or not. In many countries, the internet is, by default, free. In contrast, the internet was subject to more regulation when it was introduced in the USA than any other country in the world.

The reason is that the components of the internet were invented in the USA and they were already subject to US regulation. What is the internet? It is a network (the architecture of which was invented in the USA) made up of computers (invented in the USA) hooked up to one another through telecommunication links (of which the original was a made-in-the-USA telephone).¹

The location of invention is important. It is likely to be the location for advancement as well as use of the invention. The location would also likely be the place where the rules governing the invention would be most advanced. In this case, the rules governing the use of the components of the internet—the telecommunications, networks and computing hardware and software—are certainly the most advanced in the USA.

In many instances, the US has had no need to pass laws to prosecute offenders who use the internet as a medium to commit offenses. A classic example is the Love Bug virus case, discussed in the previous chapter. Hence, when US users proclaim that there should be no laws for cyberspace, they come from a different setting. In many developing countries, new laws are what are needed.

The framework is a guide for countries wanting to know how to begin regulating cyberspace. In general, rules regarding the internet should be formulated as the problem is being encountered. That is, the rules should not be formulated in anticipation of development of technology. There are many reasons for this course of behavior.

First, it is not easy to anticipate technological development. The US state of Utah, for example, pioneered the world's first digital signature law in 1995. Within a year, half a dozen states in the USA were modeling their digital signature law on Utah's.² That law, however, is predicated on using a certain technology. Today, it is recognized that the law needs to be changed to keep pace with technology.³ Its basic flaw is that it was too far ahead of its time and while it addressed issues current at the time the law was drafted, it does not address issues that are current today.

Second, law is at its best when it serves real-life practical problems, not some hypothesized potential problem. This is the strength of the British common law system, where law develops through cases instead of legislation. In the short-term, there can be vagueness and ambiguity in the applicability of rules. But in the long-term, the rules that emerge are more robust because they address real-life problems.

Third, because technology changes quickly, it is not possible to predict how a law may stunt and stifle instead of helping the development of technology. A classic example is the use of push technology. Around June 1997, a group of students came to the author to look into push technology for their final-year academic project. Within six months, just as they had completed data collection but even before they began writing, it was clear that push was dead. PointCast, the company that had pioneered the technology, went from US\$250 million in valuation to virtually being unsaleable. It was sold in 1999 for US\$7 million to investment firm Idealab, then buried as EntryPoint, Infogate.⁴

The following framework is intended as a guide to cover the salient issues that a policy-maker will face in drawing up legislation for a country. The order the issues are presented is likely to be the order that countries face in implementing rules for cyberspace. The precise order will likely vary according to the needs and tastes of the country in question.

A. Access and Service Provision

The first set of rules should address the basic: access and service provision of telecommunication services in order to provide internet service. Ideally, there should be competition in this area in order to drive down prices and increase consumer choice. Some regulations may be necessary to ensure fair competition if there are no competition laws. For example, the incumbent telecommunication company should not be allowed to exercise its incumbent and, where it exists, monopoly power. It should be compelled to interconnect.

On hindsight, the breakup of the American telecommunication giant AT&T under the supervision of Judge Greene, lowered telephone tariffs and contributed to the telecommunication and internet boom in America. The evidence is compelling that competition in telecommunication, by lowering prices in the near term, will spur the diffusion of the internet.

As far as possible, there should be a level playing field for internet service providers. Service providers should also be immunized from liability where it can be shown that they have acted responsibly. This point is discussed in greater detail later in Chapter 6 on the liability of intermediaries for third-party content.

B. Issues Relating To Electronic Commerce

Commercial interests spurred the diffusion of the internet. At one stage, virtually all the words in the English dictionary were being tagged for dotcoms.⁵ Therefore, ensuring that the legal system addresses e-commerce both supports businesses and leverages them to diffuse the internet. The point about addressing e-commerce issues is not that all activity in cyberspace must be commercial. Rather, the point is that by addressing these issues, one also addresses a whole host of issues that must be resolved in order for cyberspace to thrive.

For example, looking into e-commerce rules necessitates ensuring that the courts recognize and accept electronic evidence. Without electronic evidence, it is impossible to conclude a contract. As recently as the mid-1990s, in talking to officials from developing countries, I invariably encountered nationals from countries that had no law to recognize electronic evidence. This means that an e-mail offer is not admissible in court. Without electronic evidence, it is impossible to conclude a contract or to prosecute offenders in cyberspace.

A whole plethora of laws are needed to support e-commerce: authentication, digital signature, privacy, fraud protection, etc. For example as at 2001, identity theft was the number one theft complaint to the US Federal Trade Commission. The 86,168 complaints in 2001 were more double the 40,000 in 2000.⁶

Another area that would require looking into is taxation rules. The US Congress passed two moratoria to hold taxes in abeyance. States, however, are chafing. And rightly so because if the internet is indeed to be a major force for commerce, it will take away business from the offline world that is taxed. The loss of revenue must be made up somehow. Should the tax be levied at every node where the e-commerce transaction passes? These thorny issues should be resolved at an international level because some form of harmonization and coordination is probably best. And it is questionable if there are 190 experts (the number of countries in the world) who can tackle the matter with equal aplomb.

C. Content Regulation

The basic rule for cyberspace is that offline laws also apply to the online world. The major issue with regulating cyberspace content is that the laws that apply online must reconcile, as far as possible, with the offline regime.

A common, but initial, concern is pornography. In many Asian countries, pornography is simply outlawed. On the internet, however, it is difficult to block such content. Singapore and the United Arab Emirates made a symbolic gesture by blocking 100 high-traffic sites through a proxy service. Increasingly, there are also filtered services updated monthly that block pornographic sites.

Of more recent concern is where the rules are meant to protect national interests. For example, hate sites have to be blocked from access in France and Germany.

Lessig expresses the concern that the internet would be under siege from such interests. In my view, this concern is misplaced because the internet will continue to play host to fringe groups of many kinds. Nevertheless, Lessig's basic point is valid to the extent that the internet, like any communication medium, thrives best when there is the greatest freedom.

D. Security and Encryption

Security is a significant issue in cyberspace because of the extent of hacking going on. This is often the behavior of sophomore male engineering or computing students. Where they used to vent their youthful zest in physical form, they now hack into computer systems as a sign of male prowess.

The issue is not trivial. I have had the unfortunate experience of having a site hacked down to its root—the computer could not even be booted. It took the technical support person a whole Saturday to restore the system and secure the site.

Still, the nature of the internet makes it impossible to fully secure the system. Therefore some sanctions are in order to reduce such destructive behavior. There is no reason for anyone to destroy someone else's site unless perhaps as an act of war.

E. Intellectual Property Rights

The basic point here is that intellectual property rights must be extended to cyberspace. In most instances, this means strengthening the rights of holders as well. This will mean, for instance that an author who used to write for a newspaper may now be paid extra because the material is posted on the Web.

IPR, however, is tricky.

The general trend is that IPR is strengthening in favor of the rights holder. The WIPO Treaty of 1996 means that the world acknowledges the significance of IPR. A country that refuses to play by those rules will be shut out of the information economy.

However, IPR requires a balance—something noted in all literature but something that is increasingly being ignored in pursuit of financial gain.

A question is whether in the longer term, the copyright rules will hinder the development of science. Already, books, journals and databases for libraries are getting increasingly expensive.

There is little question that many countries with little intellectual property to sell have little incentive to protect the intellectual property rights of others. The USA used to be the biggest violator of copyrights. Stories abound of pirates literally rowing out to meet the incoming ship so as to beat the competition in running off copies of Charles Dickens' latest book. Now that the shoe is on the other foot, the US is attempting to protect the rights of its citizens and corporations through some not-so-subtle means.

Nevertheless, the basic point is valid that IPR has to be respected if a country is to develop its own information industry.

F. Privacy and Data Protection

Although used synonymously, these are related but not quite identical concepts. The idea is that the privacy of users should be respected so that users will come to trust cyberspace. Data protection is the means to achieving privacy protection.

The issue arises because it is computing power that makes for the heightened possibility of the invasion of privacy. That is, it was possible to find out private details about a person; but the steps were so tedious and expensive that it was just not practical. But with the computer, it is now possible to find out enough details about many people to market to them.

Privacy is a relatively new concept to many developing countries. There are many languages for which the word is a recent invention. Chinese and Malay come to mind. In both instances, the word is a recent invention.

But with the internet, there has been the heightened awareness of privacy. It is no longer possible to put the privacy genie back into the bottle.

I have put privacy last in the framework because although privacy concerns have increased, in practise a significant proportion of users seem oblivious or indifferent to it. Alan Westin's surveys of privacy indicate that privacy concerns are rising: the percentage of those he calls privacy unconcerned has fallen from 20 to 10 percent while 12 percent of the privacy indifferent have become privacy fundamentalist.¹²

Conclusion

The framework is a guide to implementing rules to make cyberspace function better. In developed countries, much of the rules are in place. For the developing countries, implementing the rules will only be playing catch up.

¹² Rick Whiting. 2002. Wary Customers Don't Trust Business to Protect Privacy. Information Week. 19 August.. <<http://www.informationweek.com/story/IWK20020816S0009>> 19 February 2003.

Policy and Legal Framework for Cyberspace

Policy and Legal Issues	Brief Description Of Concerns
A. Access and service provision	<ul style="list-style-type: none"> • How to manage technical standards in a networked environment • How to ensure interconnection and interoperability of computer systems and networks • How to regulate pricing and service quality of information services • Responsibilities and liabilities of access and service providers
B. Issues relating to electronic commerce	<ul style="list-style-type: none"> • Identification, certification and authentication of buyers and sellers, and administration of certification authorities • Legal status of digital signatures and digital certificates • Legal status of electronic payment mechanisms and electronic payments • Applicability of contract law: Rights, responsibilities and liabilities of various parties and dispute resolution mechanisms • Fraud and crime, and law enforcement in electronic commerce • Money flow and taxation in electronic commerce
C. Content regulation	<ul style="list-style-type: none"> • How to block objectionable materials on the Internet • How to protect national interests against foreign undesirable materials • How to reconcile conflicting cultural values in information content
D. Security and encryption	<ul style="list-style-type: none"> • How to protect against breaches of security in computer systems and networks • How to prevent crime in the digital environment • Rules on the use of encryption technology
E. Intellectual property rights	<ul style="list-style-type: none"> • How to manage and acquire rights in the digital environment • How to prevent piracy of copyrighted works • How to extend the current copyright regime to include digital works
F. Privacy and data protection	<ul style="list-style-type: none"> • How to protect against intrusion into individual's private information • How to control use of personal information • How to facilitate transborder data flow

¹ Michael Dertouzos in his book "What Will Be" three times credits Tim Berners-Lee with inventing the Web. But even so, Dertouzos acknowledged that it was the appearance of browsers such as Mosaic and Netscape that made it a universal phenomenon.

² Biddle, Brad (1996). Digital signature legislature: Some reasons for concern. <http://www.inet-one.com/cypherpunks/dir.96.02.22-96.02.28/msg0090.html>, accessed October 2, 2002.

- ³ Biddle, C. Bradford (1995). Digital signature legislation: Flawed efforts will hurt consumers and impede development of a public key infrastructure. *CPSR News*, 13(3), Fall 1995. <http://www.cpsr.org/publications/newsletters/issues/1995/Fall1995/biddle.html>, accessed October 2, 2002.
- ⁴ See Bicknell, Craig (March 29, 2000). PointCast coffin about to shut. *WIRED*. <http://www.wired.com/news/business/0,1367,35208,00.html>; PointCast fire sale (May 11, 1999). *WIRED News Report*. <http://www.wired.com/news/business/0,1367,19618,00.html>; Glasner, Joanna (March 6, 1999). PointCast feeling pushed out. *WIRED*. <http://www.wired.com/news/business/0,1367,18286-2,00.html>.
- ⁵ See: Glasner, Joanna (June 12, 2000). Dot Coms? They're for losers. *WIRED*. <http://www.wired.com/news/business/0,1367,36828-2,00.html>. Oakes, Chris (March 24, 2000). Tip of the dot-com backlash? *WIRED*. <http://www.wired.com/news/business/0,1367,35154-2,00.html>. Schrage, Michael (January 21, 1997). Night of the living-dead sites. *WIRED*. <http://www.wired.com/news/business/0,1367,1552,00.html>.
- ⁶ US Federal Trade Commission, Identity Theft Complaint Data. <http://www.consumer.gov/idtheft/reports.htm>, accessed, October 3, 2002. See also: Rusch, Jonathan J. (September 18, 2002). Identity theft: Fact and fiction. *CNET Tech News*. <http://news.com.com/2010-1075-958328.html>.