Issue 5, Summer 2000

WHO IS "BIG BROTHER"?

by

Giampiero Giacomello *

A. Introduction

Since its inception, the Internet has been riddled with contradictions: a communication network designed to disseminate knowledge among universities, mistaken for a Cold War device, it now carries news, data, money, and impressive sex-related material. On the Internet, one's identity can be concealed, altered, or falsified at will. This is certainly still the case; however, anonymity on the Internet has been increasing challenged by national governments. Fearful that cyber-terrorists, organized crime and pornographers could monopolize the Internet—alarming businesses and disquieting would-be users—governments around the world have started to explore ways to exercise more and more control on the Net.

The Internet, however, will not have an impact only at the domestic level, that is, within nation-states. More and more, it will also affect states' ability to run international relations as a still predominantly intergovernmental activity. In fact, should national governments decide that the Internet could really pose serious threats to their national security, they would certainly put considerable efforts into controlling it. Yet, for technically skilled individuals, escaping even the tightest controls and thus communicating with the outside world would still be possible, thus rendering such restrictions largely useless.

Perhaps international organizations, even more than states, will be affected by the seemingly unstoppable expansion of the Net. What happened with the World Trade Organization meeting in Seattle in December 1999 is a clear indication of what may lie ahead. There, activists of Non-Governmental Organizations were able to organize and efficiently run the protest—which almost led to the failure of the meeting—relying almost entirely on the Internet, and, in particular, on email and Web pages. By blurring together the domestic and international levels of communications, the Internet will soon oblige practitioners working in fields such as foreign policy analysis or international affairs to undertake a substantial revision of their trades. And scholars in the same fields will also have to take note.[1]

The Internet is a powerful communication and publishing tool for individuals whose wishes in some instances may run counter to those of other members of the society who want

* Department of Social and Political Science, European University Institute, Florence / Italy.

1 For instance, the US Institute of Peace maintains a Web Project called "Virtual Diplomacy", dedicated to demonstrate the power of new communications technologies in the international environment of the Post-Cold War world.

to preserve its social fabric and cohesion through filtering information from outside and limiting its access. Knowledge about the individuals' motivations to seek outside information may also help "social controllers" to achieve their objectives. Social control, however, varies considerably across countries as well as across time. With regard to the Internet, this occurrence means that the drive towards controlling the Net differs substantially depending on the country, or rather the government, considered.[2] And herein lies the puzzle that brought about my guiding questions: what are the causes of different national attitudes towards controlling the Internet? What explains the fact that some national governments want more control and others none?

Because of its nature as a network of networks, the Internet may resemble, to some extent, a public good, such as the oceans or the environment.[3] National leaders and their constituencies have regarded the Internet and other media as strategic tools to nourish national cohesiveness and government legitimacy, the Internet has long been left unconsidered by state bureaucracies. This fact has permitted the Net (as the Internet is familiarly called by many users) to develop without a central controlling authority which, in turn, has constituted the foremost attracting peculiarity for a coterie of would-be communicators otherwise excluded from access to the media circle.

In the past, the link between controlling information flows, exercising social control, and the manifestation of national sovereignty has been greatly treasured by national authorities all over the world, and this phenomenon has been widely acknowledged by political scientists (Saurin, 1995). As of now, in those countries that are connected to the Internet, national governments are unable to impermeabilize their frontiers to unwanted external influences of the "accidental" information highway.

No effective control of information is attainable without seriously infringing individual rights, such as the right to privacy and freedom of expression, all highly valued in democracies. The conditions of these rights in my sample of countries along with the presence of discriminative legal rules that limit Internet access on the basis of political and social considerations have been the most important indicators to demonstrate my assumptions. The preliminary results of my research are presented here.

Quantitative analysis is a powerful instrument to explore causal inference, even for non-experimental research, as is often the case for social sciences (Blalock, 1970). However, many problems could be encountered in undertaking such investigations: data are missing or of not good quality, the sample may not be entirely representative, etc. etc. These conditions are particularly true when the units of analysis are countries. Furthermore, political science scholars have only recently undertaken research on the political implications of the Internet, and at-

---

2 In this work I have used the terms government, state or country interchangeably. Although not conceptually the same, these nouns are used here to define the actual ruling elite of a given country. Indeed, I am interested in explaining what the motivations are of the ruling elites who exercise executive powers in the countries analyzed.

3 See, for instance, M. Hallgren and A. McAdams (1997) "The Economic Efficiency of Internet Public Goods" in L. McKnight and J. Bailey (eds) *Internet Economics*, Cambridge, MA: MIT Press, pp.455/478

tempts to assess the levels of national control on the Internet have been nonexistent. In addition to the scarce literature on the issue, there is more significantly no accepted *unit of measure* for Net control.

The sample for my research included 65 countries, selected with non-probability criteria—the technique is more precisely called haphazard sampling; i.e. observations are picked according to the availability of data (Zeller and Carmines, 1978). The basic "bits" of data for my observations have been national laws and regulations, information on income, education or defense spending, as well as the results from the 1998 surveys on privacy and the free use of cryptography conducted by the staff of the Electronic Privacy Information Center (EPIC).[4] Almost the entire set of data used for the quantitative analysis has been found on and downloaded from the Internet, particularly the World Wide Web, and can be easily retraced by anyone reasonably familiar with the Net.[5] In all aspects, the Net is a remarkably "transparent" object of observation for scholars studying it.

As Lewis-Beck (1995:1) points out, judgment must ultimately be exercised in properly interpreting any statistical result, especially when it comes from non-experimental social research. Given the scarcity of sources and information on this issue, applying these techniques have offered an additional, indeed invaluable, perspective to my entire research work.

Internet Control? A Tentative Definition

As mentioned earlier, the objective of my investigation is to comprehend the causes of Internet control. More precisely, I intend to explain the variation in the intensity of political control exercised by national governments on the Internet. A definition of "Internet control" is not promptly available in the existing political science literature nor can the concept be easily operationalized for measurement. Indeed, Internet control can be studied only through the observation of proxy indicators picked up by the scholar himself with the result that such choices are hardly free of any selection bias and can be very subjective—which is often the case in the social sciences.

Aware of these limits, I have developed a functional definition of *political control* on the Internet as national rules and regulations adopted by governments to limit or select individuals' access to the Net; to search and monitor on-line users' preferences and choices; as well as the prohibition, as criminal acts, of accessing specific Web pages or newsgroups, or diffusing, through Web pages, newsgroups, or e-mail information or data considered illegal by the users' law enforcement authorities. Hence, political control over the Internet can be exercised, essentially, in two ways, notably (a) *limitation and discrimination of access* to the Net (e.g. through licensing procedures based on political or social affiliation or restricting access to trusted users), and/or (b) *censorship on contents* exchanged on-line. In turn, the latter can be performed through (b1) ac-

---

4 The survey results are available at http://www.epic.org/survey/ and http://www.gilc.org/crypto/crypto-survey-99.html.

5 The dataset developed and used for my quantitative analysis will be made available on the Web (at http://www.internetstudies.org) as soon as these results are published.

tively *monitoring* the behavior of local Internet Service Providers (ISPs), and/or (b2) *screening* the various on-line procedures (e-mail, newsgroups, Web sites, etc.) utilized by private individuals to exchange information over the Net.

According to this functional definition and given the newness of this field of research, in the operationalization phase, I have selected as convincing proxies for Internet control (1) the use of cryptography, (2) the protection of privacy and (3) the number of IP hosts in the sampled countries.

(1) The *free use of cryptography* can protect individuals' private communications and prevent unauthorized access to stored information. In the words of D. Denning, "encryption can protect communications and stored information from unauthorized access and disclosure" (1997, p.172). Moreover, "the widespread availability of unbreakable encryption coupled with anonymous services could lead to a situation where practically all communications are immune from lawful interception (wiretaps) and documents from lawful search and seizure".

In the U.S. government, agencies such as the FBI and the National Security Agency (NSA) which consider the selling of the latest encryption software as a possible "threat to their national security" are pressuring Congress to enact more restrictive legislation on the use and sale of cryptography software while civil liberties pressure groups are opposed to such legislation. The fears motivating further restrictions, however, appear to be unfounded. Actually, governments, which praise freedom of speech, should not be worried if Internet users on their territory exchange communication in clear or encrypted.

(2) *Privacy and protection of personal data* are indeed fundamental individual rights, recognized in all major international treaties on human rights, and are constitutionally guaranteed in many countries. All the most important international organizations, namely the U.N. General Assembly (Guidelines concerning computerized personal data files, adopted on December 14, 1990), the OECD (Guidelines on the protection of privacy and transborder data flows), and the EU (Directive 95/46 EC of October 24, 1995) have stressed the significance of protecting privacy and personal data.

Privacy is frequently violated by governments and business which, routinely, cross-reference data from different sources. In this study I have concentrated on the former case. Given the substantial information trail that the average Net user leaves behind, it is fundamental that individuals' right to privacy is utterly protected in on-line countries to prevent governments and ISPs abuses.

(3) Finally, one of the few available indicators to estimate the size of Internet diffusion and the approximate amount of users is the *number of IP hosts* or those computers that allow individual users to access the Net. The type of Internet access can considerably vary from country to country, from simple e-mail to the full World Wide Web. The counting of IP hosts can nonetheless give a reasonable estimate of the number of computers connected to the Internet in a given country.

As a general criterion, great numbers of IP hosts in a country should indicate that national regulation authorities do not monitor Internet use and that access is relatively open to individu-

als. It is crucial to bear in mind that such a criterion is susceptible to many exceptions, but it would still be one reliable proxy for the level of control over the Net at the national level, once controlled for variables such as income distribution, education and telecoms infrastructures.

In cross-country studies such as this, the need for standardization procedures of the units of analysis is fundamental. Countries differ considerably in terms of size, wealth, and infrastructures, factors that can all affect national governments' attitudes towards controlling the Net.

Statistical packages such as SPSS allow for weighted comparisons by balancing structural variances across countries, thus facilitating the researcher in singling out the explanatory elements that are indispensable for good causal inference and viable generalizations. Equalizing countries thought the standardization of those factors guarantees that the variations in the levels of Internet control are the factual consequences of the hypothesized explanatory elements and not undesired effects due the analytic incomparability of available observations.

For controlling purposes, in the end I have selected average national incomes, the national levels of education and the numbers of telephone lines and computers available in the sampled countries (summarized as the *multimedia* indicator).[6]

B. Possible Explanations

To explain my research questions I originally devised five working hypotheses, namely:

- The *requirements of national security*, that is, "the more a state is determined to protect its national security, the more it will seek to control access by its citizens to the Internet"; many governments tend to keep their level of control over the Net from public discussion because of "national security reasons". Supperstone (1981) has noted that, since national governments control the definition of "national security", there are no limits as to what information they may decide to include into that category. This attitude of defining national security issues broadly seems quite common, although only a minority of all the countries currently on-line truly run the risk of becoming targets of information warfare related attacks. Indeed, the actual capability of inflicting serious damage to crucial national infrastructures of states is strictly limited to a small numbers of highly skilled individuals in the world who could use information manipulation as a tool for warfare. That capability is beyond the reach of the average Net user, who generally knows little of the technicalities and complexities of telecommunications and computer networks security. The vision of the "Legions of Dooms" of malicious hackers coming over the Internet is a myth often reproduced by national authorities aiming to scare the less informed;[7]

---

6 Number of telephone lines and computers per 100 people in the observed countries.

7 This attitude could be rather telling about the real intentions of some governments with regards to the Internet

- The *individualist/collectivist structures* of on-line societies or, "the more concerned with individuals' liberties (including personal communications) the state considered, the more free Internet access will be", viceversa "the more concerned for social cohesion the state considered, the more controlled access to the Internet will be". Pro-individual societies would pressure their governments to grant the most open and free access to the Internet, accepting just a minimal level of control, supporting instead self-regulation procedures, for instance;

- The *democracy level* of on-line countries, or "the more democratic a state, the greater the access to the Internet its citizens will have", and in the opposite case, "the more authoritarian a state, the less access its citizens will have to the Internet". For the democracy level as indicator for hypothesis n.3 I have used one of the indicators more commonly considered in cases like these, namely the classification of the Polity III database.[8]

- The *regulatory propensity* of on-line countries, i.e. "the stronger the historical tradition of regulatory behavior, the stronger the regulatory propensity of states considered, and the more controlled Internet access will be"; to cope with the problem of controlling Internet access and use in their territories, in all likelihood, states will fall back on their regulatory propensity towards other media and telecoms services. As a matter of fact, several governments could argue that, despite its peculiarities, the Internet does not need a special code as existing laws on telecommunications and media (press and broadcasting) already cover it. More specifically, I have considered the telecoms and media services which are either in full or partial competition or under monopoly: the higher their number, the lower the state propensity toward regulating;

- Finally, *expectations for gains from e-commerce* in on-line countries, or in other words, "the more a state expects to benefit from e-commerce and the more open its economy, the less controlled citizens' access to the Internet will be", viceversa, "the less economic payoffs are anticipated by the state, and the more closed its economy, the more restricted individual access to the Internet will be". More specifically, for this hypothesis, the type of economic approach has been paramount for the classification of the countries considered. States with open market economies and favorable to international trade tend to assure fair conditions to everybody wishing to enter the market for e-commerce, whereas states with more controlled economies may adopt regulations about on-line business that would protect specific sectors of the economy, both in industry and finance, or certain social groups or economic elite. In other words, these states would privilege the cohesion of their societies to the possibility of expanding trade and financial services with other countries via the Internet.

---

[8] The other classification commonly used is the Freedom House "Freedom of the World" annual survey (at http://www.freedomhouse.org/survey99/).

I. Test Results and Related Problems

The rules that are provided by methodology books prescribe the correct conduct by which the rigorous scholar should always be guided. Empirical observations in the real world whether of human behavior or social events, however, are rather messy and confused, as the objects of study are often enmeshed in a "noisy" cloud of contradictory signals and discordant results. Moreover, lack or inaccessibility of reliable data, coding errors, various biases, or plain misinformation by unchecked sources are the recurrent anxieties that accompany quantitative researchers—and to large extent also the qualitative ones—in all their undertakings, and my work offers no exception.

The existence of national laws limiting the use of cryptography on-line or restraining access to the Internet does *not* immediately translate into highly efficient on-line control. It does mean, though, that states *are* concerned about the possible consequences of open access to the Net in their territories. Actually, many national authorities think that "all that is not specifically permitted, is forbidden" with regard to the freedom of choice of their constituencies, and thus may want to prevent possible effects of unrestricted access to the Internet by massively regulating various on-line issues, ultimately hoping that they will be able to enforce those rules and persecute law-breakers.

The results show that the relationship among the indicators was more complex that anticipated, and they cannot be unified into a single measure for Internet control because to do so would require higher coefficients. I have considered various possible alternative explanations of why the three indicators are mildly or scarcely correlated. After all, they do represent three of the most crucial and much discussed features of the Internet.

II. Partial Correlation Coefficients for Independent and Dependent Variables[9]

	Defense	Individ	Democry	Telecomp	Econfree
Crypto	-.569**	.080	.027	.424**	-.264
Privacy	-.218	-.035	.449**	.228	-.113
IPHosts	-.148	.189	-.078	.200	.061

Table 2 (N>30; ** = 0.01 2-tailed significance)[10]

9 Controlling for education level (Educ), national income (Income), and telephone and computer infrastructures (Multimedia).

10 Defense (h.1) represent the percentage of GDP in USD devoted to defense expenditures by each countries, (SIPRI 1998); Individ (h.2) is the Individualism Index created by G. Hofstede (1980 and 1993); Democry (h.3) is indexed by the Democracy Scores (0-10)[10] of the Polity III database by Ted Gurr downloaded by ICPSR (Excel Formatted at ftp://isere.colorado.edu/pub/datasets/polity3/politymay96.data). Telecomp (h.4) is the level of liberalization/state monopoly in telecommunications and broadcasting according to the information provided by the ITU World Telecommunication Development Report 1995. See also, for instance, http://www7.itu.int/bdt_cds/IDC/Countries.idc. Econfree (h.5) is the countries' trade % of PPP GDP (1996), according to Table 6.1 of the World Bank Development Indicators 1998 (at

Given the reciprocal influence that these factors exercise on one another—which is, incidentally, also the "core business" of most social sciences—as would be expected, indications of degrees of relationship are visible for most of the indicators. The most conspicuous results are the negative correlation coefficient of *Defense* and *Crypto*, the positive one between *Telecomp* and *Crypto*, the positive one between *Democry* and *Privacy* and the negative one between *Econfree* and *Privacy*. As preliminary assessments, higher levels of defense expenditure correspond to lower scores in the free use of cryptography, i.e. the individual use of encryption software is more restricted, and vice versa, higher levels of competition in telecommunications coincide with the freer utilization of cryptography. Moreover, higher democracy levels correspond to greater protection for and care of people's privacy, while the reverse is true for higher scores of economic freedom.

First of all, privacy is a fundamental issue in the struggle for control over the Net, but the Privacy Index was based on the 1998 EPIC survey which encompassed all the aspects of privacy and personal data protection and hence the index represents the overall conditions of privacy in the observed countries.[11] Privacy protection is equally as important for the Internet as it is for the use of personal information in other media or for the treatment of individuals' health data in hospitals or in the public administration. It is then difficult to pinpoint within the privacy realm how much change is due to government control over the Internet and how much to other contingencies.

The utilization of cryptography in personal communications, on the other hand, does have repercussions in terms of protection of privacy. Unlike the Privacy Index, however, the Cryptography Index (also based on the 1998/99 EPIC surveys) may portray the conditions of Internet control more precisely. Indeed, before the diffusion of the Internet, outside of military and intelligence circles, the use of cryptography to protect personal communications was an occurrence totally unheard of; people would make phone calls or write letters knowing that the chances of their communications being read were almost nil. Many netizens today know that reading e-mail or collecting personal information on the Net is possible for any knowledgeable user—let alone national intelligence services. It is hence correct to conclude that the status of cryptography in the sampled countries can provide the researcher with a specific and more accu-

---

http://www.worldbank.org). Crypto is the condition of national pieces of legislation on the use of cryptography software for private communications from *green* (value 5 most free and uncontrolled) to *red* (1, most restricted and controlled), based on the survey conducted by the EPIC/Global Internet Liberties Campaign (http://www.gilc.org/crypto/crypto-survey-99.html). Privacy is the level of protection that personal privacy is granted in diverse countries, (http://www.gilc.org/crypto/crypto-survey-99.html). IPHosts is the ratio between the number of Internet hosts (IP-Hosts) and the population of a given country as indicated in Table 5.11 of the World Development Indicators (World Bank, 1998)

11 Privacy legislation covers, for instance, financial or health data that may not immediately available on-line but is exchanged among various institutions. If these exchanges are not regulated they may seriously infringe individuals' privacy. In this respect, the Internet may be used for collecting personal information or for cross-references.

rate indicator to measure the level of Internet control than the conditions of privacy or the number of IP host computers.

III. Explaining the Results

The low coefficients for IP host computers led me to the first important conclusion of my quantitative analysis, i.e. a low number of host computers in a given country is *not* related to government attempts to limit or discourage access to the Internet in that country. Indeed, in developing the *IPHosts* indicator, I assumed that low numbers of host computers could be the artificial consequence of national authorities trying to control the Net by imposing harsh licensing procedures and high costs to would-be ISPs. Few and expensive ISPs would then dishearten many would-be users and perhaps limit access to favored elites who may be more loyal to and supportive of the national government.

This has led me to conclude that the number of IP hosts is mainly a *function* of the level of *multimedia* that is determined by the conditions of the technical infrastructures in a country. Those technical infrastructures are, in turn, a consequence of overall national economic conditions. In section 2, commenting about the correlation coefficients of the dependent variable indicators, I concluded that at least two of them, *Privacy* and *IPHosts*, might flag some effects of government control on the Internet. However, these effects are "disturbed" by the presence of some macro-factors that influence not only the developments of the Net but also—and more importantly—the whole "social habitat" of many countries.

The highest partial correlation coefficients have been those between *Crypto* and *Defense* and between *Crypto* and *Telecomp* which has led me to focus my attention on those relationships. Moreover, the opposite signs of the two correlations appear to suggest that the two independent variables have competing effects on variations of *Crypto*. The explanation is straightforward: cryptography is essential for secure telecommunications—the fastest growing industry in the world—particularly on the Net, but, at the same time, extensive reliance on strong encryption software by individual users could put communications among criminals or terrorists out of reach for law enforcement and national security agencies. Therefore, on the one hand, various national business communities lobby for freer use (and also export liberalization in the United States) of encryption software; on the other hand, national security and law enforcement agencies and personnel pressure central governments to restrict individuals' access to that software.

In the end, four cases can thus be devised:

1) Country A has high sensitivity to national security issues (thus, high defense expenditure) but the telecoms sector is not or barely liberalized (the attitude towards regulating is high); no conflict arises as national security prevails and cryptography is restricted/controlled (e.g. Israel Ukraine or Turkey[12]);

[12] Ukraine and Turkey, however, have improved their records on the free use of cryptography in 1999 (at http://www.gilc.org/crypto/crypto-survey-99.html).

2) Country B has low defense expenditure but the telecoms sector is highly liberalized—or in the advanced process of being liberalized; no conflict arises here either, since the business logic succeeds and individual use of cryptography is free (e.g. Japan, Germany or Italy);

3) Country C has low defense expenditure and no or little liberalization in telecommunications which are highly regulated; here the conflict is irrelevant as there are no competing exigencies and the free/not free use of cryptography is a non-issue (e.g. Saudi Arabia)

4) Country D has high defense expenditure and strong liberalization in telecoms; the conflict is mostly active as the opposite pressures of the national security and business communities compete to convince the national government that cryptography should be free or not free (e.g. the United States or Britain).[13]

C. Conclusions

Extrapolating from the experience of the telecommunication and broadcasting industries, some authors (Shapiro and Varian, 1999) have argued that, as the economic importance of the Internet grows for businesses, so too will the tendency by national authorities to further regulate it. In order to be effective, therefore, regulation should anticipate methods to control on-line activities. Their speculations about the technical feasibility of strongly centralized regulation (as they seem to imply) can be contested on the basis of the fundamental difference between the nature of Internet and that of other media. The crucial difference with the Net is that control of television and radio was, from the beginning, in the hands of governments, not universities or individuals.

As demonstrated in the previous section, two indicators, *Privacy* and *IPHosts*, do show some effects of variations of levels of control on the Net but, at the same time, they also capture the disturbing reverberations caused by other social phenomena which have no or little relevance for my study. Through all this social "noise", it is rather arduous to establish to what degree the two models devised to account for changes in those two indicators can also explain variations in the levels of Internet control.

All in all, the model correlating the rival effects of telecoms competition and national security with variations in the free use of cryptography for individual communications appears to be the most viable in understanding the causes of Internet control.

The social and political factors considered in this research - democracy, national security, individualism, and regulatory propensity - have shown different degrees of influence in prompting governments to control the Internet. A notable exception to these findings is the e-

[13] Another recent example of this struggle can be France which at the start of this research had very restrictive laws on cryptography which have been recently relaxed to accommodate the requests of French entrepreneurs.

commerce expectation hypothesis that seems to be rather irrelevant to that respect. Does this outcome contradict the most important conclusion of the principal model, namely that market forces—specifically represented here by the telecoms sector—compete with national security requirements in the contest for Internet control?

The answer to that question is straightforwardly negative for the very simple reason that e-commerce is too new an occurrence of the on-line world (itself a recent invention) to produce viable indicators and data to study its impact on national economies—while this is not the case for the telecommunications sector where data are abundant already. Statistical offices in industrialized countries as well as the OECD are still in the process of evaluating how to measure e-commerce, and it will take a few years before the first datasets will be available to scholars.[14]

Unwavering solutions for other Internet problems will be necessary before firms and consumers actually embrace the Net as a viable and secure channel to conduct their business. Large use of powerful encryption software and a widespread appreciation for protection of personal data are consequently among the necessary prerequisites to promote e-commerce. Other improvements, such as better telecoms infrastructures or more extensive utilization of credit cards, are simply consequences of other, much needed social imperatives, such as more solid economic conditions and a better educated citizenry.

In this context, advanced democracies will play a crucial role in setting standards for the future development of the Internet. Or perhaps, because, despite their contradictions (and many differences), modern democracies have all become manifestations of increasingly individualistic societies, and the Internet is a communication medium that empowers individuals. Furthermore, no effective level of control over the Net is attainable without seriously infringing upon individual rights, and attempts to do so by national authorities in democratic countries would likely trigger growing discontent and opposition by their individualist societies. Ultimately, only a system of consensus self-regulation on the Net will reconcile governments and societies in democracies.

---

[14] A. Colecchia, an economist with the Statistical Office of OECD, personally confirmed this to the author during an informal talk, Milan, March 24, 1999.