Rajiv C. Shah & Christian Sandvig

SOFTWARE DEFAULTS AS DE FACTO REGULATION

The case of the wireless internet

Today's internet presumes that individuals are capable of configuring software to address issues such as spam, security, indecent content, and privacy. This assumption is worrying – common sense and empirical evidence state that not everyone is so interested or so skilled. When regulatory decisions are left to individuals, for the unskilled the default settings are the law. This article relies on evidence from the deployment of wireless routers and finds that defaults act as de facto regulation for the poor and poorly educated. This paper presents a large sample behavioral study of how people modify their 802.11 ('Wi-Fi') wireless access points from two distinct sources. The first is a secondary analysis of WifiMaps.com, one of the largest online databases of wireless router information. The second is an original wireless survey of portions of three census tracts in Chicago, selected as a diversity sample for contrast in education and income. By constructing lists of known default settings for specific brands and models, we were then able to identify how people changed their default settings. Our results show that the default settings for wireless access points are powerful. Media reports and instruction manuals have increasingly urged users to change defaults – especially passwords, network names, and encryption settings. Despite this, only half of all users change any defaults at all on the most popular brand of router. Moreover, we find that when a manufacturer sets a default 96–99 percent of users follow the suggested behavior, while only 28–57 percent of users acted to change these same default settings when exhorted to do so by expert sources. Finally, there is also a suggestion that those living in areas with lower incomes and levels of education are less likely to change defaults, although these data are not conclusive. These results show how the authority of software trumps that of advice. Consequently, policy-makers must acknowledge and address the power of software to act as de facto regulation.

Keywords Regulation; software; wireless; defaults; usability; law; policy

Information, Communication & Society Vol. 11, No. 1, February 2008, pp. 25–46
ISSN 1369-118X print/ISSN 1468-4462 online
http://www.tandf.co.uk/journals DOI: 10.1080/13691180701858836

Routledge
Taylor & Francis Group

To modern Western thinkers, which decisions require collective action and which decisions do not has always been a vexing question. At its heart lies the proper limit of government and its nature, and this heart animates debates about individualism, freedom, neoliberalism, and deregulation. When faced with any particular regulatory question, governments have always had the option of forbearance, and this option is often used as a strategy to encourage private action in the place of public action. When it is strategic, it is sometimes called 'self-regulation' or 'co-regulation', and it presumes that the government's proper role is to encourage collective or individual private action. In Internet policy this approach is ascendant in Europe (e.g. see PCMLP 2004) and the US (see Oxman 1999). A recent Council of Europe Recommendation put it starkly, recommending that all member states adopt into domestic law provisions that 'encourage the establishment of organisations which are representative of Internet actors' such as Internet Service Provider industry groups and user councils and then 'encourage such organisations to establish regulatory mechanisms' (Council of Europe 2001, Appendix) to preempt the government from doing so.

On the Internet, individual choice is also often offered as an alternative to non-governmental third parties. When considering any particular Internet policy issue in the United States it is usually assumed that the ideal regulatory solution would be individual self-determination. While scholarship has argued that 'code is law' (Lessig 1999), this position by legislators holds that code is choice. The malleability of computer software encourages regulatory forbearance, strategic and otherwise, because software can be written to provide options and defer decisions that governments would rather not consider. Given the proper tools, it is presumed that citizens are both interested in and capable of addressing any harms occurring online. This is the guiding principle for many online policy issues, such as security, indecent content, and privacy. Examples of deference to individual self-determination (or at least non-governmental solutions) are evident in software and law from the computer industry's advocacy of personal firewalls as a security solution to the legal promotion of personal filters and individual privacy 'settings' and choices in Web browser software as the solution to a dangerous internet. This isn't necessarily problematic by any means: government deference to individual autonomy or private association should be often celebrated. However, if citizens are generally unable to configure their software to address harms, talk of delegating policy decisions to 'the people' is a sham. Instead, power is being delegated somewhere else: we argue, to those who set software defaults.

This paper addresses the fundamental Internet policy preference for individual action in the US by empirically examining how often individuals change default settings in software. In other words, when users are given options, how important are the computer industry's suggestions as to what they should do? The personal experience of most computer users is sure to

include episodes of frustration when trying to configure software. Common sense might lead us to be skeptical of any scenario that depends on users changing complicated settings. However, the exact degree of skepticism we should have is also an important question, practically and morally. Practically, many sociotechnical systems require at least some users to learn to change settings so that the entire system can function. Morally, characterizing the power of default settings tells us whether deferring a decision away from government via software will ever satisfy a constituency that has a strong willingness to behave differently from everyone else. For example, if we delegate to parents the decisions about regulating Internet content that children see in their homes, we might do so out of a belief that parental autonomy and diversity in parenting styles should be respected. But if parents always accept manufacturer suggestions, we are delegating this decision to the wrong place, and no choice has really been offered. Indeed, we are really satisfying the group of parents who feel strongly enough about censorship to act (for or against) only if they have the ability to figure out how to change default settings for filters in 'Internet options' screens designed by manufacturers. That is, when deferring a choice to individuals, it may be that we are simply deferring the decision to those who decide the mechanism for choice – the designers.

This paper provides empirical evidence through a study of how individuals configure their wireless Internet (specifically, 802.11b/g 'Wi-Fi') access points (APs). Luckily, the few years after Wi-Fi's widespread introduction in 1999 provide a rare instance where a technology's settings can be measured in a naturalistic environment on a large scale during a widespread public campaign to change default settings, as we will explain. Although our analysis is relevant for those interested in Wi-Fi technology use specifically, we employ Wi-Fi here as an example of a technology where significant decisions have been intentionally left to users to make individually, rather than being collectively made by regulators, standards bodies, or hard-wired into the technology itself.

Configuration as regulation of user behavior

Concerns over software settings are not new. Scholars have widely recognized that software settings are a powerful form of regulation (Lessig 1999). This has led to the recognition that defaults play a crucial role in how people use software (Shah & Kesan 2003). While scholarly accounts agree that defaults are important, there is little empirical evidence about how powerful they are. Recent contributions by legal scholars have focused on 'settings' and 'defaults', but the notion of 'configuration' itself has also received extensive attention in the literature on Science and Technology Studies (for a partial review, see Mackay *et al.* 2000).

MacKenzie's work (1990, 1999) has shown that in technological systems the relationship between the production of knowledge and confidence in that knowledge is not linear. With the concept of the 'certainty trough', MacKenzie argued that those close to the design of technologies and those who know almost nothing about them are both likely to be uncertain about their use, function, and potential. It is those committed to a technology but not involved in its production – for instance, the users – that are most likely to express confidence in it. Woolgar (1991) elaborated that a chief task of technology designers is to 'configure' users to have certainty about their products, and that the first interaction of a potential user with a technological artifact is an instance when they are 'confronted by, and asked to engage with ... concretized perceptions of themselves' (Woolgar 1996, p. 91). To reframe this conceptualization in terms of present Internet policy debates about self-regulation, it could be said that an effort is now under way to teach Internet users fine distinctions about gradations in levels of security, privacy, and content categorization technology. The delegation of decisions about, for instance, parental censorship to screens of Web browser settings and third-party NGOs is then a way of configuring users to configure technology. Rather than seeing new settings as the logical (or the only) response to parental complaints, to borrow Woolgar's phrasing, it can be seen that users are taught that parental censorship of the Internet is an important problem, and then users are 'taught to want' personal control over content rating for their children rather than collective action or collective debate about it as a social problem. Rather than a public discussion, the chance to decide becomes a technological feature.

Approaches to studying user skill and technology use

In empirical research, the general assumption has always been that changes in defaults are directly related to a user's skill level or experience (Page *et al.* 1996). Unfortunately, in empirical studies of technology use, the prevailing method for determining a person's skill is to ask him/her to personally assess it. For example, a recent quantitative study of Internet use in the UK sought to determine the skill level of parents by asking them if they considered themselves advanced users (16 percent did; Livingstone & Bober 2005). Although this is a measure of self-efficacy, and not one of skill, this was characterized as a 'skill gap'. Survey methodologists have long mistrusted self-report measures that concern communication media (Price & Zaller 1993). Self-reports presume an ability to self-assess skills on a scale (e.g. 'novice' to 'advanced') that is anchored the same way across all respondents – a lot to ask in the context of computer ability. In addition, self-reports are subject to social desirability bias that would probably inflate

estimates of skill, and self-reports conflate other factors like 'confidence' (Svenson 1981; Taylor & Brown 1988).

Although self-reports of skill require complicated self-assessment, even survey measures that do not require self-assessment have been shown to be problematic. The methodological literature reviewed here shows that a simple question like 'Did you change the settings on your Wi-Fi router?' is probably invalid. Simply phrased self-reports about the use of communication technology that one would expect to be free from desirability bias have been shown to be surprisingly inaccurate. In the US, surveys asking for simple counts of the number of days that people watch the three largest television networks or listen to the news on the radio have been found to report 170 percent of the audience measured by audience rating services such as Nielsen and Arbitron (Price & Zaller 1990, p. 4). When social desirability bias is also strongly present, discrepancies are even more likely. Famously, in self-reports of voter turnout, as much as 18 percent of the population will falsely report that they voted (Traugott & Katosh 1979).

A more sophisticated approach is to then measure respondents in some way to ascertain technology use and/or see if they are actually skilled. Studies that have attempted this have shown that observational and/or behavioral measures of skill are far more valid than self-reports. For example, a recent Pew survey on search engines found that 92 percent of people were confident in their search skills, while 52 percent were very confident. However, 62 percent of people were not aware of any distinction between paid and unpaid search results (a knowledge test of skill) – despite the fact that the leading search engines plainly mark at least some of these results (Fallows 2005). A recent study measuring both skill and self-perceived skill found that on a four-point scale, the mean self-assessment of skill at finding information online was 0.4 (or 10 percent of the scale) lower for women than for men, even though there was no significant difference in actual skill between women and men (Hargittai and Shafer 2006).

To escape the pitfalls of survey self-reports, researchers have tested skills directly within a laboratory environment. In the most sophisticated study to date, Hargittai used a combination of surveys and observations to gauge search skills (2002, 2005; Hargittai & Shafer 2006). Kuo *et al.* conducted a usability test about setting up Wi-Fi APs using observations of users (2005). Tests in laboratory settings have shown that users often lack the capability to configure and use software. Hargittai found that users' self-perceived abilities did not reflect their digital literacy as measured by performance tests (2005). Similarly, Kuo *et al.* also found that people struggled to setup an AP securely (2005).

The sampling and artificiality limitations of laboratory tests are well known – people in the real world often act differently for a variety of reasons than they do within a laboratory. Yet even research in naturalistic settings suffers from reactivity bias – the presence of the researcher changing the

results. These limitations led us to pursue the unobtrusive measures (after Webb *et al.* 1966) that are increasingly useful in studies of the Internet (see Lee 2000, ch. 6). We thus examine when people change default settings in software using other software to collect the data. While these forms of data are often difficult to obtain, the moment of Wi-Fi use in the early 2000s provided a context where a large amount of data can readily be obtained unobtrusively from naturalistic settings – it is possible to see what defaults have been changed without asking about them. Without this approach, the investigation described here would be impossible.

Background and context: the case of Wi-Fi

Wi-Fi wireless Internet technology is a useful proxy for other, common debates about defaults and standards because Wi-Fi during the period 1999–2005 was the focus of a widespread public campaign of media reports, instruction manuals, and government reports that urged users to configure their AP securely. This typically requires people to change the default settings on their AP. As a brief background note, standardization debates within the IEEE 802.11 Working Group that designed the technology favored interoperability over security. Earlier wireless technologies had been criticized because users often found it to be difficult to get wireless devices to connect to each other, and therefore the manufacturers of Wi-Fi equipment produced consumer devices in 1999 that were open and promiscuous by default. The rushed standards process within the IEEE also advanced a security protocol that would leave security analysts wanting. This situation combined with a few sensational popular press headlines such as 'Man first in nation convicted of wireless crime' (WRAL 2003) to produce widespread discussion of wireless security settings. According to ABI/Inform *Trade & Industry*, a periodical index that includes the computing trade press, just 31 articles appeared in the year 2000 containing the name of the dominant Wi-Fi encryption protocol 'Wired Equivalent Privacy' (WEP). Just four years later 287 articles appeared in the calendar year 2004, while the database's coverage of computing industry periodicals did not increase. The theme was repeated in mainstream syndicated computer advice columns in major newspapers. A random sampling of these articles found that all of them recommended that WEP or WPA encryption be turned on and that default channel and identification settings be changed.[1]

While Wi-Fi technology was originally advanced to allow users to solve small computer networking problems in their homes, it was quickly adopted for a variety of uses and settings (Bar and Galperin 2004), becoming a rare bright spot in consumer electronics after the Internet bust and the crash of the capital markets in 2000. While the details of configuring the settings

on wireless devices may have been arcane, the relevance of these settings was not. Wi-Fi had quickly become a mainstream technology, with about 200 million Wi-Fi chipsets sold worldwide as of June 2005.[2] Wi-Fi APs operate to facilitate wireless communication, and to achieve this they broadcast some of their settings publicly to allow other Wi-Fi devices to discover them and potentially connect. This means it is possible to gather very accurate data on how people manage these settings.

Unobtrusive Wi-Fi mapping as a method

Researchers are now beginning to refer to (Schmidt & Townsend 2003) and take advantage of (Grubesic & Murray 2004; Matei & Hooker 2005) these broadcasts as a means of collecting data about wireless technology use. While the capture of these broadcasts is unfamiliar as a research method (and may at first seem to raise ethical questions), in fact logging these signals is the same process by which any laptop computer automatically determines if there are any wireless networks available nearby. Conceptually, measuring how people use wireless by logging these signals is akin to measuring the extent of the telephone network by counting telephone lines on utility poles. Both technologies provide readily accessible indications of their existence in public places if you know how to look for them. There is no expectation of privacy for these wireless signals: this can be seen in the fact that wireless encryption and security schemes exist at all – users presume that other people might find their network because this configuration information is broadcast publicly to facilitate this discovery.

We employ these data in two studies, one a secondary analysis and one a primary data collection. Of course, while unobtrusive observational measures of wireless signals are an excellent way to gather wireless settings, as a research method this cannot address how the users think about the decisions they make when changing settings. This is acceptable for our purposes only because the goal of this article is only to address the first step of determining what the consequences are of framing choices in technology settings with defaults. It is possible to observe what choices the users have been presented with by examining different Wi-Fi routers and their documentation. Then, observation of wireless signals can show how users responded to these objects.

Using data from amateur Wi-Fi mappers to consider defaults

In a little-known subculture of computer technology, the public information broadcast by APs has lately been collected by 'Wi-Fi Mappers': enthusiasts

who map out wireless networks as a hobby. These mappers share their map data with each other using free web-based geographic information systems and other software such as the Wireless Geographic Logging Engine (WiGLE) and websites like wifimaps.com. The method for collection is simply that these mappers install special software on a laptop or PDA with a Wi-Fi card, then connect a GPS device for plotting their location. The mappers then drive around a neighborhood collecting data, in a process also known as 'wardriving'. They can then produce a map that shows each AP's geographical location and attributes. For more technical details on Wi-Fi mapping see Byers & Kormann (2003). The motivations for this mapping are outside our scope here, but the useful effect of it is the creation of large databases of public information about wireless routers.

One of the most comprehensive US Wi-Fi mapping databases, http://www.wifimaps.com/, is produced by Zhrodague, a Pittsburgh, PA group of computer programmers (Sandvig 2004). It has collected data since 2003 and presently contains information on about 400,000 APs. The data it collects includes the following: the geographic location of the AP; the unique identification number of the AP (media access control address [MAC]); the wireless network name (service set identifier [SSID]); whether encryption is in use (either WEP or its successor WPA, explained below); and the channel number the wireless AP is using. The last three values are especially useful in this study, because they are modifiable by the end user of the AP. In addition, the unique identification numbers of APs can be cross-referenced with industry assignments of these numbers to determine the manufacturer of each device.

To determine whether an AP has maintained or changed its default settings, we constructed lists of known default settings for specific brands and models. We next identified those APs in the data using manufacturer-specific information that they transmit (the MAC identification number). We could then determine whether the user had deferred to its default setting or changed it by comparing the manufacturer's default value to the actual value. In the next section, we will use data obtained by agreement with wifimaps.com to analyze a number of different wireless AP attributes for nine manufacturers in the US.

Changing default encryption settings

The first issue concerns whether users used encryption. It is well understood that an unsecured wireless connection could allow unauthorized parties to eavesdrop on communication, masquerade as an authorized user, modify network traffic, and even consume network bandwidth (US General Accounting Office 2005). To prevent such unauthorized use, the 802.11b standard

includes a protocol known as Wired Equivalent Privacy (WEP). The purpose of WEP is to create an encrypted wireless communication, thus preventing unauthorized users from eavesdropping or using the network. A variety of groups from government (National Institute of Standards and Technology 2002; US-CERT 2005), manufacturers (Intel 2005; Linksys 2005), and the media (Karagiannis 2003) (Lasky *et al.* 2004) have urged people to use WEP (and later, its successor, WPA [Wi-Fi Protected Access]).

We examined 375,190 wireless APs detected in the US by amateur wireless mappers and uploaded to wifimaps.com. Mean usage of encryption across all of these APs was 30 percent. From the literature, we know that both default settings and user skill are likely to have large consequences for the way the APs we see 'in the field' are configured. We then considered the nine most common manufacturers of APs in the US (in total responsible for 242,555 of our observed APs). First, we compared the default settings of the APs to the actual settings to see how often users changed their defaults. Then, we used the target market of the wireless AP as a crude proxy for skill level. That is, some wireless devices are specifically advertised and designed for 'enterprise' use. These APs, typically more expensive than consumer models and with a better warranty and reliability rating, are marketed to IT professionals in larger organizations. There is no guarantee that IT professionals will always buy enterprise APs and consumers will always buy consumer APs, but in practice we believe that enterprise APs are very likely to be installed by IT professionals, though the picture for consumer APs is less clear. In the wifimaps.com data, we use target market as a proxy for skill by assuming that IT professionals are more likely to know something about configuring wireless routers than consumers. Table 1 presents an analysis of the data from these nine manufacturers, first grouped by default setting, then grouped by target market when default encryption setting is off. Enterprise APs are classified as Symbol, Cisco, and Agere, while consumer APs are classified as DLink, Netgear, Linksys, and Belkin.

The prediction that defaults are important is very clear. If the goal of the public discussion about encryption was to convince users to turn encryption ON, we see that simply setting the default to 'ON' produces 96 percent compliance: 3.4 times as much as setting the default to 'OFF' and exhorting the user to change the setting in the instruction manual (as these routers do). Similarly, we see routers sold to enterprises are more likely to have encryption turned on than consumer routers. It is true that these categories conflate many motives: these results are surely due to preference, awareness of the issue, and also skill at managing settings. We employed chi-square analysis to test the significance of the distributions of in these tables, first by the grouping by default setting, then in the grouping by target market. We also tested the difference between the raw percentages by manufacturer by assuming the size of the US AP market to be about 19.7 million APs in 2003. All tests found that these differences were significant ($p < 0.001$).

TABLE 1 The relationship between defaults, skill and observed encryption settings in products from nine US manufacturers.

mfr	*observed APs*[a]	*turned ON*	*grouped by default setting*[b] *(% turned ON)*	*grouped by target market*[c] *(% turned ON)*
2Wire	7698	96%	ON (96%)	
Microsoft	4131	58%	ON if setup is ever run (58%)	
Symbol	6039	55%		
Cisco	33413	38%		enterprises
Agere	30788	37%		[skilled] (39%)
DLink	19112	29%	OFF (28%)	
Netgear	20832	27%		consumers
Linksys	116797	22%		[less skilled] (23%)
Belkin	3745	20%		
overall	242555	31%		

Note. Data from wifimaps.com

[a]All percentages are statistically different ($p < .001$), assuming 19.7 million operating access points in the US in 2003 (Bar & Galperin, 2004: 53).

[b]The relationship of default settings to observed defaults was statistically significant, λ^2 (2, $N = 242{,}555$) = 115,190, $p < .001$.

[c]Among manufacturers where the default setting was OFF, the relationship between target market and observed setting is statistically significant, λ^2 (1, $N = 209{,}894$) = 23,422, $p < 0.001$.

Also, note that Microsoft's WEP usage differed significantly from the other consumer APs and was higher than any enterprise AP. This difference can be explained by the setup process for the Microsoft APs. Upon opening the box, consumers are urged to run the enclosed CD for setting up the AP. During the CD setup, WEP is automatically turned on by default. This setting differs from every other wireless AP on the market at this time. Consumer deference to this default accounts for Microsoft's AP high WEP usage. Similarly 2Wire showed the highest WEP usage of 96 percent. This high level is due to the setup process for the 2Wire AP. The setup process turns on WEP by default and even prints a default WEP key on the bottom of the unit. This forces users to go through the setup process to make the AP function at all. The result of the mandatory setup and a default setting favoring encryption is the highest WEP usage of any AP.

Changing default network names

APs always come with a default name (or SSID), such as 'linksys' for a Linksys AP or 'default' for a Dlink AP. Experts, manufacturers, and the government agencies recommend that users change this value for two reasons. The first is that hackers can recognize the default SSIDs and use them to join your network. Second, by changing the default SSID, users can prevent neighbors from 'accidentally' joining a network because more than one network within range has the same name. In addition, some users like to change their default network name as a means of personal expression (although the most common name that users change a default setting to is in fact impersonal: 'home').

Because manufacturers have different default SSID values, we again analyze the wifimaps.com data by manufacturer. Our analysis compared the number of APs using a default SSID with the total number of APs for a specific manufacturer.

The percentage of APs that changed the default SSID is shown in Table 2 by manufacturer. There are three important factors to consider when examining this data. First, there is the stark difference in the willingness to defer to default SSID values between enterprises and consumers. Enterprises are very likely to change the default SSID, with a high of 92 percent changing the default SSIDs in Symbol APs. Consumers are much more like to defer to the default SSID, with values varying from 33 percent to 45 percent. We believe the explanation for this is likely to be expertise.

Additionally, there is a again substantial difference between Microsoft and the other consumer manufacturers. This can be explained by the setup process for the Microsoft AP. Part of the setup process involves prompting users to choose a unique SSID. Users are not made aware there is a default SSID when they follow Microsoft's setup process. The 2Wire brand of APs has no unique default value. Instead 2Wire appends a three digit number to each SSID, such as 2WIRE899. This ensures that users have a somewhat unique SSID. Thus the high number for 2Wire indicates that the manufacturer has already assigned a unique setting for the consumer.

The relationships between changing one default and changing another

Of course it is problematic to abstract a concept of 'default-changing' from the context of any particular choice that technology users are being asked to make. Users change settings like default encryption because of their concerns about privacy or their predispositions for or against altruism (sharing wireless networks with strangers). We do not mean to argue that users change or do not change defaults without reference to the 'content' of the setting. Having said that, there is surely a small impetus to change more

TABLE 2 The relationship between defaults, skill and ssid settings in nine US manufacturers.

mfr	*observed APs*[a]	*changed default SSID*	*grouped by default setting*[b] *(changed default)*	*grouped by target market*[c] *(changed default)*
2Wire	7698	99%	partially unique SSID provided by manufacturer (99%)	
Microsoft	4131	72%	setup prompts user to create a new SSID (72%)	
Symbol	6039	92%	default SSID given, user must initiate any change (57%)	enterprises [skilled] (91%)
Cisco	33413	87%		
Agere	30788	96%		
DLink	19112	45%		consumers [less skilled] (42%)
Netgear	20832	41%		
Linksys	116797	41%		
Belkin	3745	33%		
overall	242555	58%		

Note. Data from wifimaps.com

[a]All percentages are statistically different ($p < .001$), assuming 19.7 million operating access points in the US in 2003 (Bar & Galperin, 2004: 53).

[b]The relationship of default settings to observed defaults was statistically significant, λ^2 (2, $N = 242{,}555$) = 72, 246, $p < .001$.

[c]Among manufacturers where the default SSID was given, the relationship between target market and observed setting is statistically significant, λ^2 (1, $N = 209{,}894$) = 51,724, $p < 0.001$.

than one setting if any settings are changed at all. When changing settings involves running configuration settings or accessing an 'options' screen or page, simply changing one setting exposes the user to all of the other settings that can be changed. It may then be useful to say that there is a kind of user that changes no settings at all because they are never exposed to the option to do so, and then there are users who are skilled enough to at least consider their options, though in the end they may not change any. The first kind of user, in the context of wireless APs, would be a user who buys a wireless device and then installs it without ever running the setup program or reading the manual. Virtually all wireless devices we measured will work 'out of the box' in this manner. To assess the prevalence of this kind of user, the next step in our analysis was to construct a count of the defaults

changed. For each wireless router, changes to three default settings can be easily measured with these data: network name (SSID), encryption (WEP/WPA), and channel (that is, frequency). This meant that the value of the index for each router would vary from 0 (no default changed) to 3 (all three defaults were changed). Table 3 shows the results for Linksys routers (the most common type) in California.

The results show that half of all Linksys routers have not been modified at all. A remaining quarter of users made one change and the last quarter of users changed two or three default values. This table supports the intuitive understanding that people are hesitant to change defaults. To assess the degree to which 'default changing' is a behavior that obtains regardless of the qualitative nature of the default, one can imagine this count of default-changing as an index and employ Cronbach's alpha, the standard lower-bound reliability estimator for indices, to quantify the degree to which changing one default is linked with the likelihood of changing more. As mentioned in the note to Table 3, the alpha is not convincing (0.57), yet even this number should be interpreted as high when realizing that each default actually controls a different function, and presumably users have different motives for changing each of the defaults. This implies that there is some reason to think about users as those who change no settings (50 percent in this example) and those who change any. Table 4 presents the inter-item correlations for this index.

A complementary study of default changing in three neighborhoods of Chicago

In the analysis so far, 'target market' is a useful proxy for skill with technology, yet the unusual nature of the source of data we analyzed so far (wireless mapping enthusiasts) and the lack of any sampling plan in the original collection we are using for secondary analysis raises legitimate questions about any conclusions drawn so far (these are also discussed in additional detail in the conclusion). For example, 'target market' is only a rough approximation of who has IT

TABLE 3 Defaults changed for Linksys APs in California.

defaults changed	*observed APs*	*cumulative %*
0	10582	50.3
1	5222	24.8
2	3914	18.6
3	1316	6.3
overall	21034	100

Source: wifimaps.com. If treated as an index, Cronbach's $\alpha = 0.57$.

TABLE 4 Pearson correlations between three default changes from Linksys routers in California.

	changed encryption	*changed name*	*changed channel*
changed encryption	1	0.39**	0.19**
changed name		1	0.34**
changed channel			1

Note. Source: wifimaps.com. **$p < 0.01$.

skill. Whatever validity we may have gained by using unobtrusive, behavioral, non-reactive measures arguably may have been lost in error for this operationalization of skill – there is no way of knowing that products sold to enterprises really indicate skill level. To address these concerns, we conducted a small original data collection using similar wireless mapping methods in Chicago.

We selected three census tracts in Chicago to form a diversity sample, maximizing variation in income and education. When compared with all census tracts in Cook County, these three tracts represent the poorest community area, the richest community area, and a community area with near average income.[3] Researchers then selected a census tract in each community area such that land use was as similar as possible across all three tracts – each tract selected had to include residential buildings of varying densities (from apartments to freestanding single-family homes), mixed-use commercial/residential areas (businesses on the first floor with apartments above), and commercial areas (office buildings, stores). Due to the effect of building material on wireless signals, all three areas must be of predominantly brick construction. Due to the effect of street layout on signal propagation, all three selected tracts had to have a grid pattern of streets. In short, although we are again using unobtrusive observations in a naturalistic setting, in this portion of the study we tried to control for the most obvious confounds that might compromise the wifimaps.com data. To obtain original data, the same researchers visited the census tract in each area with standardized equipment and drove on every street within an area of approximately 0.5 km^2 in each tract.

Let us very briefly introduce the three sample neighborhoods at this point. The first tract, Humboldt Park, is one of Chicago's poorest – in the 6th percentile of median household income citywide. Humboldt Park is known for its large Latino and Black populations, and the tract we observed has been identified by the police as one of the highest-priority problem areas in the city for violent crime. The second tract, West Ridge, is very ethnically and racially diverse: home to an established immigrant community of South Asians, an enclave of Orthodox Jews, and others. Median per capita income of the tract is in the 35th percentile, and the area is known for ethnic restaurants and as a shopping destination. Third, the Lake View neighborhood is in the 97th

percentile of median household income in Chicago, and this is the community area where the largest percentage of the young, male population works in IT-related occupations, according to the 2000 US Census.

We compared default-changing behavior for Linksys routers, the most popular manufacturer of routers observed in all neighborhoods. The means and standard deviations for each neighborhood are reported in Table 5, where an analysis of variance (ANOVA) revealed statistically significant differences.[4] The very low instance of Wi-Fi AP use in the poorest neighborhood (Humboldt Park) does not allow us to generalize about this neighborhood.[5]

In this analysis, our measure of skill is the percentage of residents in the tract who have obtained a high-school diploma, and our measure of wealth is the per-capita income reported to the US Census in 2000. The design of this study does not allow us to distinguish between the effect of income and education (normally collinear in any case) but it does allow us to note with a small sample ($N = 713$ Linksys routers) that the poorer neighborhood (West Ridge) with less education and a higher minority population changed fewer defaults. The difference between these neighborhoods is small but significant for West Ridge, and it bears out the same relationship to skill using a very different measure than the wifimaps.com data.

Limitations of this study

There are several limitations with this analysis. The first few analyses were secondary studies of data from WiFiMaps.com. These data were not collected with any recognizable sampling plan, and we believe there are significant biases in the resulting sample. For example, the mappers tend to oversample interstate highways, high traffic roads, affluent areas, and metropolitan areas. In short, this dataset is only likely to include data from areas where the kind of person who

TABLE 5 *Defaults changed in linksys Routers in three Chicago neighborhoods.*

	per-capita income	*% with H.S. diploma*	*% white*	*observed APs*	*defaults changed*[a]
Humboldt Park	$9060	56.1	1.0	16	1.4 (.62)
West Ridge	17573	80.6	64.6	137	1.5 (.80)[b]
Lake View	54280	94.8	85.5	560	1.8 (.83)[b]
overall				713	1.7 (.83)

Note. Demographics from US Census 2000, network measurements from 2004.

[a]Mean (S.D.) on a range from 0–3.

[b]Only groups with this superscript were statistically different by Bonferroni posthoc comparison ($p < .001$) to the ANOVA results reported in the text.

likes to do amateur wireless mapping is likely to drive. As wireless mapping itself is an expensive hobby (requiring a laptop or at least a handheld computer and significant computing expertise), this means that wifimaps.com data will dramatically under-represent poorer neighborhoods. At the time of our first data collection in Chicago, Wifimaps.com contained no data for our three Chicago neighborhoods. We believe these biases do not affect the analyses we conducted on wifimaps.com data, but we can never fully characterize this unusual source of data. Second, our study of neighborhoods measures not the income, education, or race of the purchasers of the routers, but the mean values for the census tract where they live. Census tracts are large areas and in this study each tract ranged in population from 4,125 to 8,945 residents. A mean across this range is likely a very crude measure of the same value for our 713 wireless AP users.

All of the statistical analyses presented for the wifimaps.com data are problematic because these analyses assume random sampling that did not exist. In addition, our need to understand the categorical distinctions endemic to default settings limits the statistical methods available to us to nonparametric tests like the chi-square. The very large dataset then makes any difference likely to be statistically significant, but its substantive meaning may be affected by the collection biases just mentioned. We have tried to address these problems by including our own smaller, original data collection. However the nature of our object of study – wireless routers – confounds wireless diffusion and default settings in our three-neighborhood study. That is, users in areas where there is more Wi-Fi are more likely to need to change default settings like encryption, network name, and channel as there are more Wi-Fi users near them who threaten their privacy, can interfere with them on the same channel, or are likely to misidentify someone else's network as their own. Since we are interested in income and education and these are primary determinants of who buys wireless routers (note the few APs found in Humboldt Park), it is not possible to eliminate this confound in the design of this study. Additionally, we cannot make claims about income as distinct from education or race (or any other neighborhood characteristic) because our naturalistic setting cannot isolate these variables.

Finally, we attempted to analyze the relationship between income and education in the wifimaps.com data using techniques similar to our own study of three neighborhoods in Chicago, but we could find no relationship – we attribute this to the sampling bias of the wifimaps.com data and its under-representation of low-income areas.

Implications: the false choice of user self-determination

Our results show that default settings play a powerful role in how people use technology. People are hesitant to change the manufacturer's default settings

and defer to them. While this argument is well known to scholars in this area, this study found empirical evidence to quantify this effect using multiple measures from two very different sources of data (one of them very large). In our empirical study, we found that most people do not change default settings. Specifically, we found that when a manufacturer sets a default setting to 'ON', 96–99 percent of users follow the manufacturer's suggestion. When a manufacturer sets a default setting to 'OFF', and users are exhorted to change the setting by the media, instruction manuals, and online help, only 28–57 percent of users will do so. About half of the users of the most popular product changed no defaults at all, and there was a small positive association between changing one default setting and changing another, even though the qualitative nature of the default settings we considered was quite different. There is also a suggestion that those living in areas with lower incomes, lower levels of education, and higher minority populations are less likely to change defaults, although these data are not conclusive due to the limitations of our design – further research on this final point is needed. Finally, all data in this study were gathered unobtrusively, with no overt interaction between participants and researchers, allowing triangulation with other studies employing more common survey and experimental methods.

Practically, our results also cast doubt on whether education or public awareness campaigns directed to the general population can ever encourage users to behave differently if manufacturers and technology designers do not act to assist them in doing so. After all, consumers in this instance have been pushed to change wireless AP default settings by manufacturers, government, and the media. Nevertheless, the majority of consumers did not do anything.

The results here lead us to sharply question the conventional policy approach in the US and EU when Internet policy and technology regulation is at issue. In these debates, the relevant decision is often framed as a decision between government action and inaction; regulation and forbearance; or public vs. private action. In answering the question 'Should government act?' regulators assume that answering 'no' (inaction) can be equated with individual freedom, choice, or proxy action by expert groups (such as ISP associations or user representatives introduced at the beginning of this paper). For example, content regulation strategies like the Platform for Internet Content Selection (PICS) were originally endorsed by regulators because they were to give users the freedom to make their own 'regulations'. This forbearance is always attractive when a decision must be made about something where there is little consensus and strong feelings – as for example the control of indecent Internet content in the US. The empirical data show, however, that regulatory forbearance is really leaving the choice to manufacturers and technology designers, even when they develop elaborate technologies (like PICS or WEP) that are meant to empower their consumers.

In terms of law and policy, this has important normative and practical implications. It implies that many situations described by the words 'deregulation', 'unregulation', 'no regulation', and 'regulatory forbearance' are often instances where decisions have really been left to industrial 'best practices' and the software designers that choose defaults – often, it seems, with little deliberation. Users are given the illusion of choice, but are unlikely to have the time, awareness, or skill necessary to actually choose anything. The largest implication of this is that self-regulatory strategies in this mold do not move debate and discussion from the public to the private sector; instead they probably preempt debate entirely. Conceptualizing choice as a technological feature in this way actually allows someone else (in this case, manufacturers and designers) to make these choices. This also means that the terms 'co-regulation' and 'self-regulation' that usually apply to regulatory schemes where industrial actors are dominant are actually much more prevalent than they appear.

Once the power of default settings determined by manufacturers is recognized, the solution becomes clear. Default settings must become the object of attention. This has happened to some degree in debates about 'opt-in' vs. 'opt-out' privacy protection schemes, but this thinking needs to be broadly applied to any arena where a choice is being deferred away from public debate – any arena where choice becomes a feature. It is true this shift of focus may be unpopular for policy-makers – forbearance allows policy-makers to avoid making a decision about controversial topics, while the regulation of defaults demands a decision even if that decision is not mandatory for all users (though in practice, we have seen that some defaults are effectively mandatory).

Attention to default setting does not necessarily call for more government action. In the case of consumer APs, both Microsoft and 2Wire used their control of the user interface to force users to make explicit decisions when designers thought explicit decisions were necessary. This sort of approach can be promoted by many different actors beyond government.

The broadest point to be taken from this research is to remind us that individual self-determination has limitations. In all cases people have limited resources and interest in configuring technologies. Consequently, it is necessary to push and prod developers to set default settings that comport with established societal concerns. After all, developers do understand that defaults matter. In a 2005 decision, Microsoft opted to change a default setting in the latest version of its operating system so that a firewall is now turned on by default (in Windows XP Service Pack 2), greatly increasing the number of users who have a firewall and increasing the security of all computers.

This consideration of defaults is immediately relevant to a variety of pressing public policy issues. For example, default settings about Web

browser cookies and RFID chips will determine what personal information is shared by users and what is private. Similarly, default settings for filtering technology from Web browser content ratings to television's V-Chip surely play a significant role in the overall flow of communications. Accessibility of communication to the disabled also frequently succeeds or fails because of default settings in the software that produces the communication – as the accessibility of Web pages is determined by the default settings in the Web authoring software that encourage or discourage authors to design communications in an accessible way. This is another case where attention must be focused on default settings provided by manufacturers, or deference to third parties, co-regulation, or 'individual freedom' is really deference to software designers and a way of not talking about a technological and political decision with important consequences.

In sum, a general rule might be that the authority of software trumps that of advice, and that conceptualizing choice as a feature is a way of avoiding a difficult public debate. For effective social control of the difficult choices surrounding the introduction of new information and communication technologies, there must be consideration of how defaults are set by manufacturers, and this is empirically more important than the goal of simply facilitating 'choice'.

Acknowledgements

This material is based on work supported by the National Science Foundation under Grant No. 0308269 and 0546409. The authors would like to thank Drew Celley for making the data from wifimaps.com available to us and Dave Chan, Rivka Daar, James Kinzer, Siddhartha Raja, and Ryan Spain of the University of Illinois at Urbana-Champaign for the collection of wireless data in Chicago.

Notes

1 Admittedly, there are even more effective security and encryption settings that advanced users can take that do not involve WEP or its successor, WPA. For example, very advanced users may not bother with WEP (or WPA) because they are seen as relatively weak. Instead, they may opt to encrypt all traffic using a virtual private network. This strategy is not detected in our data, but we believe it to be rare.

2 This is a very rough estimate based on press releases. For example, see http://www.broadcom.com/press/release.php?id=725298. Chipsets includes both access points and Wi-Fi cards.

3 'Community Area' is a historically useful geographical unit consisting of several census tracts. Community Areas are specific to Chicago.

4 $F(2, 40) = 7.82$, $p < 0.001$. As the group sizes varied significantly, Welch's variance-weighted ANOVA was also conducted, but did not produce any distinguishable difference.

5 Bonferroni posthoc tests revealed that the difference between Lake View and West Ridge was significant. No other posthoc contrasts were significant.

References

Bar, F. & Galperin, H. (2004) 'Building the wireless internet infrastructure: from cordless ethernet archipelagos to wireless grids', *Communications & Strategies*, vol. 54, no. 2, pp. 45–68.

Byers, S. & Kormann, D. (2003) '802.11b access point mapping', *Communications of the ACM*, vol. 46, no. 5, pp. 41–46.

Council of Europe (2001) Recommendation Rec(2001)8 of the Committee of Ministers to member states on self-regulation concerning cyber content. [Online] Available at: http://cm.coe.int/ta/rec/2001/2001r8.htm.

Fallows, D. (2005) 'Search engine users', Pew Internet & American Life Project, [Online] Available at: http://www.pewinternet.org/pdfs/PIP_Searchengine_users.pdf (25 January 2008).

Grubesic, T. H. & Murray, A. T. (2004) '"Where" matters: location and Wi–Fi access', *Journal of Urban Technology*, vol. 11, no. 1, pp. 1–28.

Hargittai, E. (2002) 'Beyond logs and surveys: in-depth measures of people's online skills', *Journal of the American Society for Information Science and Technology*, vol. 53, no. 14, pp. 1239–1244.

Hargittai, E. (2005) 'Survey measures of web–oriented digital literacy', *Social Science Computer Review*, vol. 23, no. 3, pp. 371–379.

Hargittai, E. & Shafer, S. (2006) 'Differences in actual and perceived online skills: the role of gender', *Social Science Quarterly*, vol. 87, no. 2, pp. 432–448.

Intel (2005) 'Wireless Network Security Resource Center'. [Online] Available at: http://www.intel.com/personal/wireless/security/index.htm (12 July 2005).

Karagiannis, K. (2003) 'Ten steps to a secure wireless network', *PC Magazine*, 25 February, p. 64.

Kuo, C., Perrig, A. & Walker, J. (2005) 'Designing an evaluation method for security user interfaces: lessons from studying insecure wireless network configuration', *Interactions*, May–June, pp. 28–31.

Lasky, M. S., O'Reilly, D., Dahl, E. & Steers, K. (2004) 'No-hassle wireless networking superguide', *PC World*, February, pp. 138–140.

Lee, R. M. (2000) *Unobtrusive Methods in Social Research*, Open University Press, London.

Lessig, L. (1999) *Code and Other Laws of Cyberspace*, Basic Books, New York.

Linksys (2005) 'Protecting your wireless network'. [Online] Available at: http://www.linksys.com/servlet/Satellite?childpagename=USpercent2FLayout&packedargs=cpercent3DL_Content_C1percent26cidpercent3D1116519873380&pagename=Linksyspercent2FCommonpercent2FVisitorWrapper (12 July 2005).

Livingstone, S. & Bober, M. (2005) *UK Children Go Online*. [Online] Available at: http://personal.lse.ac.uk/BOBER/UKCGOfinalReport.pdf (22 January 2008).

Matei, S. A. & Hooker, J. F. (2005) 'Wireless networks: social capital, diffusion, and encryption practices'. Paper presented to the 6th annual meeting of the Association of Internet Researchers, Chicago, Illinois, USA.

Mackay, H., Carne, C., Beynon-Davies, P. & Tudhope, D. (2000) 'Reconfiguring the User', *Social Studies of Science*, vol. 30, no. 5, pp. 737–757.

Mackenzie, D. (1990) *Inventing Accuracy: A Historical Sociology of Nuclear Missile Guidance*, MIT Press, Cambridge, MA.

Mackenzie, D. (1999) 'The certainty trough', in *Society on the Line: Information Politics in the Digital Age*, ed. W. Dutton, Oxford University Press, Oxford, pp. 43–46.

National Institute of Standards and Technology (2002) *Wireless Network Security*, NIST, Gaithersburg, MD, pp. 800–848.

Oxman, J. (1999) *The FCC and the Unregulation of the Internet*, Office of Plans and Policy Working Paper No. 31, Federal Communications Commission, Washington, DC. [Online] Available at: http://www.fcc.gov/osp/workingp.html (22 January 2008).

Page, S. R., Johnsgard, T. J., Albert, U. & Allen, C. D. (1996) 'User customization of a word processor', paper presented to CHI 96, Vancouver, BC Canada, 13–18 April.

Price, V. & Zaller, J. (1990). *Evaluation of Media Exposure Items in the 1989 ANES Pilot Study*, ANES Pilot Study Report No. nes002283. [Online] Available at: ftp://ftp.electionstudies.org/ftp/nes/bibliography/documents/nes002283.pdf (22 January 2008).

Price, V. & Zaller, J. (1993) 'Who gets the news? Alternative measures of news reception and their implications for research', *Public Opinion Quarterly*, vol. 57, no. 2, pp. 133–164.

PCMLP. (2004) *Internet Self-Regulation: An Overview*, Programme in Comparative Media Law and Policy IAPCODE/selfregulation.info Research Project Report, Oxford University, Oxford. [online] Available at: http://www.selfregulation.info/iapcoda/030329-selfreg-global-report.htm.

Sandvig, C. (2004) 'An initial assessment of cooperative action in Wi-Fi networking', *Telecommunications Policy*, vol. 28, nos 7–8, pp. 579–602.

Schmidt, T. & Townsend, A. (2003) 'Wireless networking security: why Wi-Fi wants to be free', *Communications of the ACM*, vol. 46, no. 5, pp. 47–52.

Shah, R. C. & Kesan, J. P. (2003) 'Manipulating the governance characteristics of code', *Info*, vol. 5, no. 4, pp. 3–9.

Svenson, O. (1981) 'Are we all less risky and more skillful than our fellow drivers?', *Acta Psychologica*, vol. 47, no. 2, pp. 143–148.

Taylor, S. S. & Brown, J. D. (1988) 'Illusion and well being: a social psychology perspective on mental health', *Psychological Bulletin*, vol. 103, no. 2, pp. 193–210.

Traugott, M. W. & Katosh J. P. (1979) 'Response validity in surveys of voting behavior', *Public Opinion Quarterly*, vol. 43, no. 3, pp. 359–377.

US General Accounting Office (2005) *Information Security: Federal Agencies Need to Improve Controls Over Wireless Security*, GAO-05-383, US General Accounting Office, Washington, DC.

US-CERT (2005) 'Cyber security tip ST05-003 – securing wireless networks'. [Online] Available at: http://www.us-cert.gov/cas/tips/ST05-003.html (12 July 2005).

Webb, E. J., Campbell, D. T., Schwartz, R. D. & Sechrest, L. (1966) *Unobtrusive Measures: Nonreactive Research in the Social Sciences*, Rand McNally, Chicago, IL.

Woolgar, S. (1991) 'Configuring the user: the case of usability trials', in *A Sociology of Monsters: Essays on Power, Technology, and Domination*, ed. J. Law, Routledge, London, pp. 57–99.

Woolgar, S. (1996) 'Technologies as cultural artifacts', in *Information and Communication Technologies: Visions and Realities*, ed. W. Dutton, Oxford University Press, Oxford, pp. 87–102.

WRAL (2003) 'Holly Springs man first in nation convicted of wireless crime'. [Online] Available at: http://www.wral.com/news/2612619/detail.html (23 September 2005).

Rajiv C. Shah is an Adjunct Assistant Professor in the Department of Communication at the University of Illinois at Chicago. He received his PhD from the Institute of Communications Research at the University of Illinois at Urbana-Champaign. Prior to that he earned a JD from the University of Illinois at Urbana-Champaign and a BS in Electrical Engineering from the University of Nebraska-Lincoln. *Address*: Department of Communications, University of Illinois-Chicago, 14 Brownstone Ct., Bloomington, IL 61704, USA. [email: rshah@a5.com]

Christian Sandvig is an assistant professor in Speech Communication at the University of Illinois at Urbana-Champaign where he studies communication technology and public policy. Sandvig received the PhD in Communication from Stanford University. *Address*: 244 Lincoln Hall, University of Illinois, 702 South Wright Street, Urbana, IL 61801, USA. [email: csandvig@uiuc.edu]