Objective Subjectivity: Behind Artifacts' Assertation of Intentionality

Rowin Andruscavage

April 11, 2001

S&TS 438 SP01 Paper 2

Bruno Latour shows that doors and other artifacts act as constant constraints upon human behaviour. Though they are mere mechanisms, their sociological effects are indistinguishable from moral or normative control. As they often perform the task of human agents, we have an inclination to assign these objects the intent of their conscious counterparts. By design, the purpose of these artifacts is to regulate our behaviour in such a way as to create and preserve social order. Imbued with these traits, such artifacts become the minions of an absent but overseeing authoritarian figure known only proverbially as "The Man." Accordingly, people have a tendency to develop negative feelings towards these devices and sometimes vent their frustrations on them, in the meantime subverting aggression away from the real culprits, the human designers, manufacturers, or governing bodies, for better or for worse. Taking a look at the motivations behind an object's design will give us clearer insight into the object's purpose, or what might be regarded as its true intent.

The Boundaries of Moral Control

Everywhere one travels, we can see the general population subjected to the moral controls of the fiercely territorial human race. We've erected walls and fences everywhere possible to keep out trespassers and would-be thieves, performing the duties of guards constantly reminding people to respect one another's property. These obstacles are not insurmountable, of course. As guards might be distracted or bribed, so too could walls be forced open or

bypassed, and fences scaled or burrowed under. The difficulty with which these barriers yield to force or subversion speaks of the degree to which the owner wants to keep perpetrators away. Some fences are so easy to cross that their presence is merely symbolic, such as the little stone garden borders or white picket fences that convey the message: "Please don't step on the petunias." This ranges to the menacing prison barricades topped with electrified barbed wire and adorned with signs showing a silhouette figure buckled over backwards from shock: "You're not getting through here alive." Somewhere in between are the curious class of apparently civil fences topped with ornamental spikes. To the casual onlooker they're frivolous pieces of architecture, but to persons harbouring intentions to climb the fence they're a thinly veiled threat of bodily harm. The efforts of the architect to conceal the harsher message of the fence behind ornament perhaps belies our reluctance to accept and openly display the primal territorial urge that we share with some animals. However, even when the objectivity of a fence is stripped down to the bare minimum of a "No Trespassing" sign nailed to a tree, its intention remains prevalent. Though physical barriers no longer exist, the mere threat of beration or litigation or perhaps even an imagined encounter with a shotgun-toting Uncle Lenny gives enough impetus for most of us to keep out.

Bruno Latour gives an excellent treatise on the intricacies of door sociology in his article on "Mixing Humans and Nonhumans Together: The Sociology of a Door-Closer."[1] Therefore, this paper will only endeavour to extend his argument to that of locks. Like walls and fences, locks keep thieves and vagrants from trespassing into private space unwarranted, with the added complexity of allowing only individuals endowed with the right key to pass through somewhat freely. This has the effect of associating the value of one's worldly possessions to the key, an otherwise uninteresting slab of cheap metal. Especially since most locks do not distinguish between the rightful bearer of the key and an imposter, possession of the right key subverts the intended purpose of the lock and counteracts its message of moral control. If the guard allows us to pass, would we not feel more inclined to do so? Most will pass the opportunity, out of consideration for the owner, but still, when presented with an unattended running vehicle or a vending machine left open, we feel invited (by the lock, even) to have a joyride or partake of a free snack. Key possession, by association, empowers the individual with access to all under the corresponding locks' protection, whether moral or not.

[1] *Social Problems*, June 1988

Artifactual Normative Control

Several artifacts also exert a form of normative control over the population. Some walls and fences act to direct traffic smoothly along prescribed paths. Large supermarkets, department stores, and theatres often arrange separate entrances and exits in such a way as to aggregate and streamline the traffic flow. Escalators travel in one direction. Doors and locks on public buildings limit accessibility to the hours of operation. Most of this normative control is actually pretty transparent... until it fails for some reason. The supermarket layout becomes quite inconvenient if you realize that you left your wallet or purse in your car upon entering. If the entrance doors don't allow you to backtrack, you might find yourself walking halfway through the store around a long shelf that separates the entrance from the checkout lanes. Some supermarkets might be designed this way to deter thieves, since all persons and merchandise would be required to leave through the monitored checkout aisles. But often that somewhat awkward layout is inspired by the supermarket chain's desire to subject you to as much advertising and impulse-buy opportunities as possible, especially as evidenced by the product placement on the racks in the checkout lane. Most stores take a break and close for the night, though, and they lock their doors to indicate this to their incoming customers. The locks usually save them from the task of turning away customers personally, as some of them can get quite desperate. In a sense, the locks are discriminating against night owls, or those who just get off work late, encouraging them to adapt to a more common schedule. Or perhaps the store does not want the business of the type of person who stays up late. This may not be the issue in the United States, where the advent of the 24-hour convenience store has taken prevalence. However, other parts of the world (such as Germany, where almost all commerce shuts down at 6PM!) may leave the night owl stranded. The biggest discrimination traditionally has been against the handicapped, who would often be unable to use escalators or other conventional means of access. However, thanks to extensive equal access legislation, modern buildings are constructed with universal design in mind, meaning that people in wheelchairs or families with strollers will always find alternate paths of ramps and elevators to get to their destination. This is becoming especially important at a time where current projections of the population predict a dramatic increase in the proportion of elderly people in the U.S., since life expectancy is up and the baby boomers are hitting the age of modern maturity. By the year 2030, the nation will have an age demographic

much like that of Florida today.[2] Combined with the fact that they will control a large percentage of the economy's disposable wealth, stores should find it financially as well as legally imperative to extend the big friendly blue handicapped access button to their patrons. Of course, the handicapped may still be out of luck in the event of a fire when the elevators are subsequently deactivated, so there's still ample room left for improvement.

Across The Digital Divide

Computers too have their equivalent mechanisms for asserting moral and normative control. Firewalls, ports, and keys combine to protect what we call "intellectual property," or IP, in somewhat the same way that walls, doors, and locks protect your real property. Likewise, computers have issues catering to elderly users with impaired vision or hearing, but they're not quite as prepared for universal access.

Firewalls are security devices used to protect a local area network of computers from the rest of the Internet. A firewall is usually a computer itself that sits on both the internal and external networks and restricts/regulates traffic between them. It's main purpose is to make sure none of the thieves and trespassers on the Internet can come in and steal or interfere with data inside. Most computer operating systems have rather weak security, so if an attacker has direct Internet access to it, they can generally break in by exploiting a known weakness in an offered service. The firewall has quite strong security since they are designed as special-purpose systems that don't offer any service at all. However, a firewall also typically serves as a gateway, through which authorized individuals inside can access data elsewhere on the Internet. They might also be configured to selectively let only a few services through in either direction. This is the case with what is known as The Great Firewall of China, which is the censorship mechanism that The People's Republic of China uses to keep their citizens enshrouded within the iron curtain of communism. This firewall prevents people in China from viewing politically sensitive news reports not controlled by the Chinese government.[3] However, the system's has about the same effectiveness as the original Great Wall, which means that people can circumvent it easily. Safeweb.com provides one such service, which allows people to access information via proxy and have that information

[2]Census Bureau on U.S. Population Growth, http://usinfo.state.gov/topical/global/populate/00011303.htm
[3]The Great Fire Wall of China, http://www.e-businessworld.com/english/crd_internet85253.html

transmitted back encrypted so the government filters won't catch it. The service is available through a multitude of volunteer sites throughout the world, so the government cannot simply block all of them through their firewall. So outside influences are able to pass through the Iron Curtain in some fashion or another.

The concept of software keys are somewhat similar to their metal counterparts, except that they more often protect the software company's intellectual property rather than your own. The keys have traditionally served as crude anti-piracy copy protection measures. They often consist of a set of numbers that the user enters upon software installation. The keys merely act as an activation code and does not necessarily have to be unique for the user; in fact any valid key for the software will do. Generally, the keys are not used for anything identifying the user other than for registration for technical support, so they hardly serve as a barrier for copy protection. As such, software piracy has run rampant, especially in regions with low disposable income, such as China and college campuses. Users have nothing against sharing product keys since they give up none of their own property in doing so (things would be much different if you shared house keys). The moral controls against trading software are currently near nil, so the software powers that be have developed new copy protection technology that should significantly raise the bar. Microsoft will deploy one such system with its new "XP" line of products. First of all, the new keys will be unique for a certain user's name and also computer hardware, rather than just distributing a set of generic keys with the software installation media. Second, every computer will be required to check in with the company over the Internet for renewal, or else the programs will prevent the user from creating or editing their files.[4] It has yet to be seen whether this business model will be successful at reducing piracy or even retaining customers, since even the best copy-protection schemes of the past have been superceded, and these measures introduce legitimate customers to unprecedented inconvenience. All software copy protection has been broken in the past, primarily because it's usually not a difficult thing for an experienced hacker to do. It simply boils down to finding the binary software "flag" that determines whether a program is authorized run or not and tricking it into thinking that it's up. Furthermore, generic activation keys almost always exist for large corporate customers, and these will tend to leak out. On the other hand, customers will be forced to cope with these new moral controls

[4] Microsoft Challenge: Sort through FUD on Microsoft product activation, http://www.techrepublic.com/article.jhtml?id=r00220010308bot01.htm

and find even more software difficulties when trying to upgrade their computer, change their user name, or find that their software has changed after connecting to the Internet. The last company that attempted a similar scheme was Circuit City with their DivX digital video format, which required a video player to contact the licensing center every time a DivX video was played to check for payment information. Needless to say, this scheme was a complete market failure due to the availability of the competing DVD format.[5] Microsoft may have more luck due to their monopoly position, but they may be underestimating the current availability of viable alternatives.

Other ways the computer industry has recently proposed to add moral controls to software objects include the Secure Digital Media Initiative (SDMI), spearheaded by the Recording Industry Association of America (RIAA). This technology will attempt to protect copyrighted audio and video media from unauthorized reproduction and distribution. Music watermarked with this technology could only be played with special license-aware hardware and software that will refuse to allow access to the original digital encoding before playing the degraded analog signal to the speakers. As an efficacy test of these controls, the industry challenged the cracker community to see if they could gain unauthorized access to the original music data protected by an early version of the watermark. Despite a grassroots boycott of an effort to essentially help the media conglomerates improve their system, several parties went ahead anyway and cracked the code within a matter of a few months,[6] so the industry has gone back to trying to improve the holes in their technology. Of course, the cracker community is confident that any such scheme should be as easily broken has it has in the past. SDMI differs little from the CSS encryption used ostensibly to protect DVD video data. However, the control provided by the DVD encryption codes doesn't exactly prevent copying to a VHS tape or even another recordable DVD. Instead, they contribute more to the establishment of "region codes," which correspond to DVD player hardware sold in different countries. The overall effect is that DVD movies bought in the U.S. market will not play on European DVD players, allowing the recording companies to make separate releases in foreign markets and charge different price scales in each. This type of market control just happens to be illegal under international trade regulations, but the media conglomerates get away with it under the guise of an ineffectual moral copyright infringement control. This

[5] DIVX: New Convenience or Digital Disaster? http://coverage.cnet.com/Content/Gadgets/Guides/Divx/index.html
[6] deSDMI, http://www.julienstern.org/sdmi

has led to a proliferation of underground 'mod chips' which circumvent the region codes of most DVD players, allowing them to play any DVD released for any market. This has also led to an interesting court case, in which the recording industry took legal action against a 17 year old Norwegian who managed to write a CSS decryption program in order to allow DVDs to be played under UNIX-like operating systems (which currently still do not have access to appropriately licensed DVD software). The corporation sued to have the program source code removed from the Internet for violating a clause of the DMCA (Digital Media Copyright Act) which makes such decryption code illegal to publish. The judge awarded an injunction against publishing the source code to deCSS on the Internet,[7] which has led to a massive civil disobedience response from the internet community. DeCSS now has the distinction of being the first code deemed illegal, so free speech advocates have been having a field day challenging this ruling with museums of alternate ways of distributing this code.[8]

To illustrate the intensity of legal activity being spearheaded on the Internet, it is enlightening to imagine the real-life counterparts to the development of moral controls on the Internet. An artist has created a chair that operates on a per-seat license scheme similar to that used for some common software products. The chair comes equipped with a magnetic stripe reader for credit cards or another form of ID. Upon activation, a set of spikes retract from the seat of the chair and allow the customer to sit down while the device plays music and displays the end user license agreement from a monitor. After a period of time, the monitor flashes a warning indicating that the seat's license is about to expire. A few seconds afterwards, the steel spikes protrude, and the credit card machine awaits the next victim... er customer.[9]

Normative Computer Controls

The computer industry applies just as many, if not more, normative controls to their end users. Proprietary software formats lock users into relying on particular software programs, such as Microsoft Word. The formats get changed with every release of the software, so that users who refuse to buy the new version find that they can no longer read files sent to them by their associates using the new format. Additionally, new versions of software invariably

[7] DVD/DeCSS: MPAA Wins In New York, http://slashdot.org/yro/00/08/17/1827208.shtml
[8] Gallery of CSS Descramblers, http://www.cs.cmu.edu/~dst/DeCSS/Gallery/index.html
[9] Seating made simple(tm), http://wearcam.org/seatsale

require more hardware resources (even for the same functionality), forcing computer users to upgrade their hardware along with their software. Becoming a computer user enters that user into a vicious cycle of upgrades required to stay up to date with the latest format norms.

Interestingly, the users can resist some of these changes and in a way assert their own control over the computer industry. Both Netscape and Microsoft have made their bids at trying to "enhance" email communication using their own formats (HTML and .doc, respectively). However, the overwhelming backlash from the masses of people who use and rely on plain old text email has seemed to have stalled their effort into making Netscape Communicator or Microsoft Word a necessity for reading and writing email.

In order to ease the distension between the ever-escalating circle of normative control between the computer industry and the increasingly discriminating end users, the industry has agreed to work out standards for themselves. These standards define file formats and communication protocols that allow disparate products to interoperate. This gives the user a selection of products to perform a task, such as browse the Internet. More importantly to the industry, this also allows new technologies to be adopted by a large user base faster, thus avoiding the long, costly, economically stagnant wait-and-see approach that cautious users take when deciding which of several competing technologies to buy (witness VHS vs. Betamax). However, even once a product claims to adhere to a standard, the company still often finds it advantageous to "extend" the standard with proprietary features. If these features catch on in the marketplace, that gives their product the edge over their competition, simultaneously launching everyone back into the vicious upgrade cycle (the formats that define the world wide web are still mutating rapidly because of this effect). Companies that succeed at these tactics end up with a monopoly position over the market, leading to a failure of the normative control the user base can exercise back at the industry with their power of choice. Thus, the public must resort to other means of restoring competition, such as by pursuing legal regulation (of course, legal "proceedings" proceed with such sluggishness that changing market conditions usually puts an industry giant in its place by the time the justice department is ready to apply punitive measures, as was the case with IBM back in the 80's).[10]

Of course, the technological world provides just as many unintentional normative controls. As with the real world, software designers often ignore the plight of the handicapped,

[10] Justice Department Decides to Break Up Microsoft, http://slashdot.org/articles/00/06/07/2015223.shtml

and fail to create programs that could be operated by blind or deaf users. Oftentimes they break interoperability for silly aesthetic reasons by replacing button text with graphical icons which not only obscure their function to normal users, but also prevent text-to-speech programs from giving a blind person a shot in the dark at navigating an interface. Computing technology also creates economic barriers. The industry has accustomed us to the notion that computer hardware over 4 years old is long obsolete, and usually no longer runs current software acceptably. Therefore, we've maintained the notion that a decent computer system costs upwards of $1000, even when large corporations and educational institutions are literally throwing away their "antiquated" hardware (which, with properly tuned software, could be perfectly capable of giving low-income families a perfectly usable system for well under $100). Instead, those without their own Internet access would subscribe to "free" Internet services that bombard them with advertisements for products which they'll probably not buy anyway, or experience the Internet only through public libraries where government-mandated filtering software tells them that it is not moral for them to view the web site of the Women's Liberation Organization for some undisclosed reason. Equal access free of normative controls still remains a lofty goal in the online world.

Conclusion

So when is a cigar just a cigar and not a malicious health risk intent on seducing a smoker with addictive chemicals and exploiting South American farmers working for slave wages? According to anti-corporate advocates, never, not as long as a greedy manufacturer stands behind its production. Whether or not their devisers intentionally imbued the objects we encounter in our daily lives with a sociological presence, we can accept Latour's argument that they affect our behaviour. The extent of their effect varies largely with our willingness and ability to adapt, however. And our background knowledge allows us to identify the real culprits behind the apparent intentions of the objects we deal with. When we accidentally break through the drywall in our house, we don't tend to blame the wall lacking the constitution to support and protect us; we accuse the building contractors of using cheap building materials.

Incidentally, Latour's test for imagining human counterparts to artifacts fails somewhat when we consider the privacy that walls provide. We would find it difficult to entrust a

human being with ensuring our privacy while we go about our daily business; they couldn't do the job a fraction as well as walls that surround us could. If anything, those humans would become the source of all gossip! At least we can trust inanimate objects to stick with the limited states of intention which they've been designed to assert, no more, no less. We can trust walls implicitly in this respect.

The same cannot be said of the computer artifacts we encounter, however. Software is an ever-changing beast by nature, and the changes can will only get more intrusive and insidious now that companies are beginning to update the products on your computer without your knowledge transparently over the Internet. Changes can just as easily creep into our hardware. Increasingly, software vendors are entering into technical partnerships with hardware manufacturers to supply stricter controls. Storage manufacturers have been attempting to standardize a scheme for implementing copy protection on a very low level, ostensibly below a code cracker's ability to circumvent copy protection using software. If the recording industry continues to have their way, we can foresee a time when we'd have to lock ourselves alone in a soundproof room in order to "experience" copyrighted materials. Privacy invasions are already common today, where certain programs such as Earthlink[11] versions of Internet Explorer have been found to report extra information (allowing them to sell your personal profile to direct marketing agencies or for other, more nefarious uses). Intel at one point had tried to introduce a CPU ID into their processors, which would similarly allow companies to track individuals.[12] In all of these cases, the parties involved have been forced to provide patches to restore privacy to the users, but only once these violations had been publicized. The computer, which once provided users with unparallelled anonymity on the Internet, have begun to reverse its role into one of the most invasive agents of the corporation and even of the government.

The computer world is clearly setting new standards in moral and normative control. Unfortunately, legislation regulating the extent of this control is lagging precisely because of the impact these controls already have. Because computer documents including email form part of a legislator's public record and thus compromises their privacy, lawmakers often forego computer usage while in office. Ironically, this isolates lawmakers from the problem, meanwhile letting corporate policy set the standard. Thus, in the near future, we can imagine

[11]Shields Up!!: The Composition of EarthLink's Custom Browser Token, http://grc.com/su/earthlink.htm
[12]Intel Nixes Chip-Tracking ID, http://www.wired.com/news/politics/0,1283,35950,00.html

a time when these now-ridiculous practices will be used as precedents for increasing control over our lives in the real world, for better or for worse.