Piracy and the Problems of Information Policing

Adrian Johns

NYU, January 2013

As many here will know, in 2009 (actually early 2010) I published a book called *Piracy*, which purported to trace a history of information larceny from about 1650 to 2000. It is still a little early to say what impact, if any, the book will have, but the most interesting experience to occur to me so far in its wake took place in Venice. *Piracy* had been translated into Italian, and its publication coincided with a large conference for booksellers that took place in the city in late January 2011. I was invited to come and give a talk about piracy, which I did. What puzzled me was the level of interest shown by the Italian media: I found myself doing interviews with many newspapers and radio stations, the political character of which ranged from socialist to Catholic. The interviewers were generally extremely well informed, and asked difficult, probing questions that required a lot of thought to address. *La Repubblica* even published the speech. All this attention was very flattering, but it was also something unfamiliar to me; in Great Britain (my birthplace) and the United States, while I had appeared in various popular media over the years, I had never received this kind of sustained public scrutiny. What was going on?

In the end I asked a few of the interviewers that question. The answer I got was common to everyone I asked: it had to do with Silvio Berlusconi and Wikileaks. Julian Assange's website was in the news in late 2010 and early 2011 because of its scoops on US military policy, among other subjects. At the same time, in Italy the antics of the Berlusconi government were exciting discussion about the future shape of politics itself. The point was that Berlusconi seemed to pose an agonizing problem of principle for Italian social democracy. Traditionally, democrats, in Italy as in other countries, had placed great faith in the freedom of the press: with a free press, the argument ran, a government's bad actions would eventually become known, and the people would vote it out of office. But with Berlusconi as Prime Minister, freedom of the press meant freedom for Berlusconi himself, in his *alter ego* as media baron. So social democrats were looking to Wikileaks as the potential prototype for a new politics. If freedom of the press had become implausible as a bulwark

for a good society, they wondered, could freedom of *information* take its place? Could a principle that all information should and could be freely circulated without the mediation of industrial middlemen become a new political axiom? They were searching in *Piracy* to find the ingredients of a new politics.

As it happens, I am rather a skeptic about the more extreme claims made for information libertarianism. Wikileaks has done good things, but that does not make it a model for politics in general, because it elides what seems to me a desirable distinction between secrecy and confidentiality. But the point I want to make here is simply that the Italian commentators were absolutely right to press these questions. The history told in the book *is*, in the end, political history – of a kind. Indeed, the problem to which piracy gives rise today, far from being something unique to the age of genomics and big data, is a political problem of the grandest, most traditional sort.

The reason for this is that the emergence of piracy has been a long story, albeit one in which we have reached a new chapter. Today, the political character of the information society is being worked out through a series of contests, large and small, local and global, many of which can be represented as bids to define a boundary between pirates and anti-pirates. I want to focus here on what I take to be two of the most significant developments: the flourishing and convergence of private and public enterprises dedicated to combating piracy and counterfeiting; and the rise of explicit resistance to such efforts, of which Wikileaks, Anonymous, and the pirate parties that have arisen in various countries are only the most prominent examples.

*

Behind both anti-piracy and public resistance lies the enduring presence of piracy itself, of course. Estimates vary widely, but last year the International Chamber of Commerce guessed its annual cost to the world economy to be $1tn. And there is evidence that the most egregiously criminal forms of piracy, at least, are changing. As digital networks have become the preferred means for accessing and transferring information, so the street-level practice of CD and DVD piracy seems to be declining in favor of network piracy. The practice changes with an all-network medium, and not simply because of the Internet's obvious characteristics of near-instantaneity and minimal distribution costs. Since its origins in the early modern period, piracy has often been a cross-border activity, and the Internet allows this activity to ramify in new ways because it changes the status of

borders themselves. For example, a pirate group distributing access to television channels may have a corporate base in one country, an audience in several others, and a p2p (or equivalent) system distributed across even more, with the content residing stably in no one jurisdiction at all. The implications are profound because this kind of practice has no presence that is constant or substantial enough to be tackled by a conventional police effort. (That is a real example, by the way, confronted by Hong Kong police a year or two ago.) The traditional jurisdictional boundaries of police forces become entirely inappropriate. Policing becomes a matter of creating "on the ground" hybrid networks of agencies, corporations, technologies, and norms that provide for the practical monitoring and interdiction of these kinds of networks. As so often, formal institutions, laws, and policies lag behind these practical alliances.

We need better knowledge of all this – not only of piracy, but of anti-piracy too. And we need a different *kind* of knowledge – one far more attentive to social, cultural, and historical distinctions, and far more sensitive to how local contexts can shape each side and its effects.

On the anti-piracy side this is a matter of the "intellectual property defense industry." This industry has expanded and consolidated since 2009-10. It is to a significant extent a knowledge enterprise in its own right. The defenders of intellectual property see their task as one, not of police actions per se, but of three strategic activities: training, standardization, and technological development. It is clear that, at many levels from the very local to the global, participants in this industry view these as their key endeavors – more important, for example, than the grand seizures of pirated DVDs that still sporadically draw journalistic attention.

Both public agencies and private corporations declare that training local police to notice and act upon piracies is at least as important to them as actually hunting pirates down. They act on this assumption. Companies seek to liaise with local police and encourage them to notice when products are being counterfeited, for example. The acme of the approach is represented by the new phenomenon of "colleges" devoted to educating anti-pirate forces. Two in particular stand out. One originated in 2006 at the US Patent and Trademark Office: a "Global IP Academy," it trains overseas officials *in situ*, often employing active US enforcement agents from the FBI or other agencies as teachers. The other is an "International IP Crime Investigators College" (IIPCIC) aligned with Interpol. By mid-2012 this "fully interactive online IP crime training facility" had

"graduated" almost 800 officers from 14 countries. For the most part the "education" provided by such bodies is fairly elementary and task-centered. It sometimes amounts to little more than pointing out the existence of laws and the possibility of their being infringed and enforced. At a more sophisticated level it aspires to standardize "best practices" involving the gathering, handling, and deployment of evidence, the conduct of seizures, and the like, across national and institutional boundaries. The most important aspect of all, however, is probably not anything represented in the *formal* offerings of an "academy" or "college" at all. Training, especially if done face-to-face, may serve to establish informal social links across agencies, nations, or the public-private divide that may be drawn upon later when action may be on the cards. The same is true of the regular international conferences bringing anti-pirate forces together, which now attract hundreds of participants from across the world. Again, two series of these are especially prominent: the annual International Law Enforcement IP Crime Conference, the most recent of which occurred in Panama City in September 2012, and the Global Congress on Combating Counterfeiting and Piracy, last held in Paris in February 2011 and next convening in Istanbul in mid-2013. Both are organized as collaborations between public agencies and private corporations in the IP defense industry.

The consolidation of this industry helps to explain the current rhetoric of antipiracy. Strictly speaking, such rhetoric is often about counterfeiting rather than piracy. That is, it focuses on concerns about authenticity, trust, and credit, rather than on the economic costs of replicating software, music, or movies. And the point at issue is often explicitly public health: "piracy" causes a breakdown of trust in pharmaceuticals, for example, which matters because people die, whether from taking counterfeit drugs or from distrusting authentic ones. This rhetoric is not just for external consumption. Within the IP defense industry itself, talk centers on the risks posed by counterfeit medicines, foodstuffs, and automobile and aerospace parts. The kind of counterfeiting tackled by the World Health Organization's IMPACT group is elided with the kind of piracy tackled by, say, the RIAA. At the same time, the rhetoric focuses insistently on the networked and cosmopolitan character of this "piracy." It is one aspect of international "organized crime." As such, the IP defense industry maintains, piracy and counterfeiting are major sources of funding for drug-smuggling and even terrorism. Actual evidence for the consistency of these links is hard to come by, and does not seem to circulate very plentifully in the industry itself, but the representation itself is consistent and appears to be widely credited by insiders. (It was invoked by many

participants at the 2012 Panama Conference, for example, from workaday detectives to the President of Interpol itself; I heard nobody question it.)

It is easy to suggest self-interest as a reason for advancing these representations: presumably, passing laws and creating policies against piracy will be easier if the public in a given region believes that the target is a shadowy international crime syndicate in league with Al-Qaeda rather than Kim DotCom, and that the immediate beneficiaries are local children rather than multinational corporations. And one of the more notable developments since 2009 is that, after the failures of SOPA and PIPA, and probably ACTA and HADOPI too, this is now a genuinely consequential consideration. But although this kind of suggestion circulates among some digerati, it is hardly satisfactory. It fails to account for the prevalence of the representation within the IP defense industry itself, and it collapses what is in fact a complex, diverse set of communities into one interest group. Indeed, it may be that one effect of aligning piracy with counterfeiting in the context of public health is to reinforce standardization *within* the IP defense industry.

In this context it is worth noting that Interpol's preferred approach is currently not to identify piracy/counterfeiting itself as a prime target at all. It recommends instead viewing it as one example of a broader category of Trafficking in Illicit Goods (TIG), where "goods" could include any kind of commercial entity up to and including human beings. This has two implications. One is that it defines the offence in terms of trans-border movements. "Piracy" now becomes a practice the international character of which is as essential as the violation of intellectual property. It is therefore something that has, almost by definition, to be perpetrated by "international criminal networks." Policing too must consequently supervene the jurisdictional restrictions of national police forces, and become a reflection of these networks, hybrid and versatile. Correspondingly, Interpol now champions "Trafficking in Illicit Goods and Intellectual Property Crime Training Seminars," nine of which took place in 2011 alone, with 500 officers participating from 30 countries. The second implication is to strengthen the association between piracy/counterfeiting and crimes that are much more unambiguously matters of public detestation, such as drug smuggling and sex trafficking – and terrorism.

This redefinition in terms of networks coincides with some of the grander aspirations for a technological solution to piracy. If piracy is really a branch of TIG, then the same technologies can

serve to combat it as are used to secure supply chains. One obvious instance is radio-frequency identification (RFID) tagging in the domain of pharmaceuticals. A more recent example is Interpol's own "Global Register," which would collect information from manufacturers for authenticating would-be counterfeits. Unlike Interpol's separate "Database on International Intellectual Property Crime" (which is restricted), the Global Register would apparently "empower the public, rights holders and law enforcement officials by enabling anyone with a mobile phone or Internet-connected device to verify a product's legitimacy." It was unveiled at an event held under the aegis of none other than Google in mid-2012 on the theme of "Illicit Networks: Forces in Opposition" (or, with typical neatness, INFO) – a title that captures the current self-representation of the anti-pirate police.

The promise of an anti-pirate technology has often been found enticing. One part of the story of the intellectual property police since around 1980 (and in some ways for decades longer) has been the quest for some such device. But no such solution has ever been found effective, and the disadvantages of register-based approaches are not difficult to see. Take, for example, the most prominent use to date of RFID tracking in pharmaceuticals. A system of this kind was adopted for the controversial painkiller oxycontin in the mid-2000s. It was originally meant not so much to detect pirated (that is, counterfeit) oxycontin as to track *legitimate* batches of the drug which might have been stolen or misdirected. In principle, anyone with a scanner and access to the system could trace the path of a given batch immediately, and therefore implicate thieves or, it was claimed, counterfeiters. But RFID in itself does not prevent copying, of course: it could do so only within elaborate social and technological networks that are intricate and expensive to maintain. (Think of the problems of checking for errors in such an information ecology, and then, perhaps worse, of actually correcting them.) It requires additional local information of unpredictable kinds: for example, a drug shipment may require supply-chain details capable of being verified only by legwork. In effect, RFID could work as an anti-counterfeiting technology only if a conventional anti-piracy policing culture already existed. And, banally but crucially, RFID tags attach not to medicines themselves but to their containers. So what the system really tracks is plastic packaging – packaging that is, in fact, routinely replaced by intermediary companies in legitimate supply chains. All of this is in addition to the fact that for years RFID tags themselves had high failure rates. The head of Novartis's global corporate security operation summed all this up in testimony to the US Congress in 2005 and warned of the consequences.

> Counterfeiters generally deal, not only with counterfeit product, but with diverted, expired, and stolen product as well. Envision the scenario where a counterfeiter steals product, removes genuine product from the 'secure packages', and then puts the counterfeit product in these packages, and then reinserts the counterfeit product back into the system. The counterfeit product would pass through all the readers successfully. What then happens to the genuine product? The irony is that the genuine product would most likely be repackaged in counterfeit packaging with unreadable tags and entered into the distribution system. If the RFID system works *correctly*, the genuine product would be kicked out of the system, but later determined to be genuine, *undermining any confidence in the system*.

What we see articulated explicitly here is the problem of credit – of trust – that is central to issues of piracy and anti-piracy, and that has reappeared in different forms throughout a history extending back at least as far as Robert Boyle's attempts to validate medicaments. *Plus ça change*: as one industry watcher has remarked, "ultimately the consumer will still be relying on… trust in the local apothecary." If anything, the exaggerated promises made for digital authentication systems like RFID or Interpol's GR cast those old problems into even sharper relief. To be sure, such systems may eventually work as anti-counterfeiting technologies, albeit fallible ones. They may be the least-worst way of addressing a problem that is insoluble because it is fundamental to the very institutionalization of an enterprise like pharmaceuticals as, at root, informational. But they will work only if embedded in elaborate legal, social, institutional, and technological infrastructure. Their success in fighting piracy would come at the cost of constrictive implications in other domains, because they must involve surveillance, information gathering and management, checking protocols, and centralization. There have even been concerns that RFID has privacy implications because a pharmacy's technology could 'read' the identity of any drug in a customer's handbag.

These network-plus-detector systems are one branch of an increasingly baroque armoury of anti-pirate technologies. We have devices and codes such as the infamous "digital rights management" protocols, which are designed to prevent piratical copying (and, all too often, *any* copying). We have others that seek to detect when copying has taken place. Online, simplistic algorithms automatically identify apparent copyright infringements and send take-down demands, all without human intervention – resulting in absurdities like NASA having to remove footage of its own Mars landing. And a genetically engineered organism may be crippled, say, if its use cannot be

guaranteed as legitimate, where "legitimate" is defined by the corporation owning the patent. Such anti-pirate tech embodies a promise to provide an automated solution to "piracy," and is always insensitive to the complexities of everyday practice. The trouble is that the problem it addresses is not, itself, fundamentally technological; it is economic, political, and cultural – in a word, historical. As a result, anti-pirate technologies promise to make IP strong, and do, but at the expense of making it brittle. (E.g.: one of the more enthusiastic backers of networked authentication is the tobacco industry, which touts its own *Codentify* system. The ironies of this industry standing for the defense of public health and trust do not need to be belabored.)

*

One of the IP defense industry's greatest successes has been the stream of legislative measures and treaties that have appeared in the last generation, and that in recent years have become so controversial. Bills like the Stop Online Piracy Act and the Protect IP Act (SOPA and PIPA) in the United States, the ill-starred HADOPI measure in France, the Digital Economy Act in Britain, and similar measures elsewhere draw a great deal of media attention and increasingly excite opposition. So do international agreements like ACTA and, now, the Trans-Pacific Partnership (TPP). The 2011-12 campaign against SOPA/PIPA in particular, which culminated in the demise of both bills only months after they had seemed set for easy passage into law, may well be a turning point. The apparent rejection of ACTA, too, shows that public anxiety about excessive IP enforcement is not a phenomenon restricted to the United States.

The public furor that focuses on each successive bill or proposed treaty is important, but it is also to a certain extent misdirected. Such measures ought to be recognized as second-order events – as responses to problems. They typically come about because the IP police are *already* taking measures that such legislation would ratify. Specifically, they arise after initiatives to uphold and/or extend some anti-piracy strategy hit a difficulty, typically in the courts. Historically, anti-piracy practices have often tested legal bounds, and judges have occasionally stymied them. Early examples mentioned in *Piracy* include courts' refusal to embrace the London book trade's anti-pirate campaign in the mid-eighteenth century and the skepticism that judges displayed toward the music industry's "commandoes" in the early twentieth. In each case, as today, the frustrated anti-pirates attempted to

achieve through legislation what they risked losing on the ground. It is the increasing coherence of the IP defense industry that makes the process so inexorable today. And new laws, of course, set the conditions of possibility that will provoke the *next* campaign for new laws. In focusing so avidly on new legislation, therefore, the public tends to miss what propels it forward – the practical culture of enforcement. That means that an opportunity is missed too, because practical strategies are sometimes visible in a way that closed-door policy negotiations are not.

The enduring legacy of all these moments of public resistance may be represented by the proliferation of pirate parties. Such parties now exist in many countries, and since 2010 they have been united under a Pirate International. In several nations they have won representation in political assemblies: Germany, the Czech Republic, Spain, Austria, and Switzerland all now have public representatives from their respective Pirate Parties, and the Swedes – who invented the form in 2006 in the wake of controversy over the attempted suppression of the Pirate Bay – have sent Pirates to the European Parliament. In other countries, including France, Great Britain, and the United States, pirate parties exist but are thus far of little significance, probably because the electoral systems of those countries make third-party or single-issue campaigns almost always exercises in futility. Overall, it seems likely that the pirate party movement is not a flash in the pan: it has already experienced sufficient electoral success and shown sufficient political sturdiness to make that unlikely. Its more probable fate will be to follow the trajectory of Green parties in many of the same countries a generation ago. Like the Greens, the Pirates have a serious point to make, with consequences for all of us, and one that does not map readily onto traditional left-right political distinctions. They are therefore likely to see their arguments adopted opportunistically by the large mainstream parties. That may well be frustrating to the pirate partisans, but in historical terms it would be a real achievement – perhaps a greater achievement than the emergence of an otherwise ineffective digital-culture "third way" would be. The politics of IP skepticism have at least as long a history as IP itself, extending back through 1930s New Dealers to the partisans of the Scottish and French Enlightenments. But they have lacked this kind of commitment, and have tended to lose. The pirate parties may help to change that.

*

India has been the location of some notably enterprising approaches to digital media, alleged piracy among them. In 2010 Bollywood announced that it would begin "using pirate tactics to beat the pirates." It would employ what it called "cyber hitmen" to attack websites distributing unauthorized movies, including the Pirate Bay. A company named Aiplex Software was hired to discover these sites, send cease-and-desist notices, and attack the 5% of bit-torrent sites that ignored the letters. So the company's software began trawling the Internet looking for tell-tale links to new movie files. When it found them, it would send two formal notices. If this did not lead them to remove the material, Aiplex would launch Denial of Service (DoS) assaults to cripple the sites, and at the extreme even try remotely to destroy the files themselves.

A DoS attack, however, is a problematic strategy for the defenders of propriety to adopt. It involves clogging a target site up by sending millions of requests for responses at high speed. It is not quite the same as a *distributed* Denial of Service attack (DDoS) – the weapon of choice at the time for hacker groups like Anonymous – but the two are similar in approach, and both are illegal in some countries because they damage computer networks. The tactic is certainly controversial enough that some copyright enforcement organizations disown it. Worse still, it attracts retaliation. In response to Aiplex's DoS attack on the Pirate Bay, Anonymous launched its own DDoS attack against Aiplex, using a "Low Orbit Ion Cannon" system. It was one of the actions that inaugurated the notorious collective's "operation payback," which ended up targeting many corporations and institutions deemed to harm digital freedom. Anonymous's attack swiftly took down Aiplex's site, before moving on to assault the MPAA and RIAA and, later, corporations like Mastercard that had acted against Wikileaks. The conflict is still continuing at the time of writing, but it was already evident by 2011 that things were not going all the IP defenders' way.

You can find similar stories to this in any branch of the global information economy today. They raise genuine questions about the role and implications of piracy and intellectual property policing. Far from the contest between clearly distinct moral absolutes that is portrayed by both sides, some newly-arrived alien anthropologist would find it very hard to tell good guys from bad. Even Anonymous's one-time weapon of choice, the Low Orbit Ion Cannon, was in fact originally devised by the cybersecurity industry as a tool for testing network defenses. In appropriating it, Anonymous turned its own technology against it. The real question is where *this* reality came from – and why the public indifference to it?

To answer that question, we need to appreciate the history, not just of piracy itself, but of piracy and its antagonists. By now that history has shaped the mundane realities of information itself. It shapes how digital and other resources can be obtained, moved, and put to use – on an everyday basis, by all of us. That is why the question that *Piracy* ends with, "Who will guard the guards," remains so essential. And the reason to be concerned about it is *not* that the IP defenders are necessarily wrong in believing their controversial practices necessary, nor that they are fighting a war against progress. On the contrary, the reason to be concerned is that they may very well be right. Perhaps information *can* only be protected by making compromises elsewhere in the complex social contract of late modernity, and perhaps those compromises should indeed be made. The question is where we should draw the line. We should be well advised to approach that question with an appreciation of what is at stake and how things got to be this way. The prospects for reconciling intellectual property with the good society may depend on that.