2015

From Anonymity to Identification

A. Michael Froomkin
University of Miami School of Law, froomkin@law.miami.edu

FIELD OF FOCUS 4
SELF-REGULATION AND REGULATION
INDIVIDUALS AND ORGANISATIONS

UNIVERSITÄT
HEIDELBERG
ZUKUNFT
SEIT 1386

Journal of Self-Regulation and Regulation

Volume 01 (2015)

From Anonymity to Identification

A. Michael Froomkin

Abstract

This article examines whether anonymity online has a future. In the early days of the Internet, strong cryptography, anonymous remailers, and a relative lack of surveillance created an environment conducive to anonymous communication. Today, the outlook for online anonymity is poor. Several forces combine against it: ideologies that hold that anonymity is dangerous, or that identifying evil-doers is more important than ensuring a safe mechanism for unpopular speech; the profitability of identification in commerce; government surveillance; the influence of intellectual property interests and in requiring hardware and other tools that enforce identification; and the law at both national and supranational levels. As a result of these forces, online anonymity is now much more difficult than previously, and looks to become less and less possible. Nevertheless, the ability to speak truly freely remains an important 'safety valve' technology for the oppressed, for dissidents, and for whistle-blowers. The article argues that as data collection online merges with data collection offline, the ability to speak anonymously online will only become more valuable. Technical changes will be required if online anonymity is to remain possible. Whether these changes are possible depends on whether the public comes to appreciate value the option of anonymous speech while it is still possible to engineer mechanisms to permit it.

Keywords

Internet, Privacy, Anonymity, Surveillance, Speech

DOI: 10.11588/josar.2015.0.23480

From Anonymity to Identification

A. Michael Froomkin

1 Introduction

This is not a cheerful paper, which mirrors the lecture from which it is adapted.[1] It is not cheerful because the prognosis for effective online anonymity has become progressively less and less cheerful.

By anonymity, I mean something strong: the ability to speak without anybody being able to identify you. This untraceable anonymity is the highest level of technical protection for speech (cf. Froomkin 1995). That it is untraceable brings with it the ability to speak without fear of jail, harm, or other retaliation. This strong version of anonymity is controversial. The arguments for why untraceable anonymity is a good thing include the idea that it contributes to human flourishing; people want to experiment, and the ability to experiment with less fear contributes to human self-realization. In places that are less free, avoiding retribution for saying the wrong thing may be a matter of life and death. Political dissidents, ethnic minorities, religious splinter groups, people campaigning for women's rights or gay rights, and many others are, or have been, subject to the risk of genuine and very palpable violence. If they wish to speak or write for their causes they need a means to protect themselves. Anonymity is one such tool.

For those of us who do not face the danger of personal violence in retaliation for our writings, there are nonetheless other more subtle dangers. One is the danger of profiling. Profiling enables stereotypical discrimination on the basis of sexual orientation, political opinion, or other characteristics. Less serious, but annoying, is the effort commercial entities make to profile for marketing purposes.

Anonymity is a way to defend against that profiling, a protection that is desirable not just because some find it creepy or uncomfortable to be profiled, but also because the people doing the profiling could actually exercise market power by doing price discrimination (DeLong et al. 2000).

When the Internet started, one byproduct of the architecture of the Internet was that online anonymity was easy to achieve. It required only minimal technical knowledge, or fairly simple tools, or assistance from the right people. In those days you

1 The lecture from which this paper is adapted was delivered at the University of Heidelberg on Dec 11, 2015, under the auspices of the Netzpolitik AG of the University of Heidelberg. I am very grateful to Dr. Wolf J. Schünemann and all my hosts for the invitation and the warm welcome. Unless otherwise noted, this paper attempts to reflect legal and technical developments up to May 1, 2015.

could be anonymous and have a great deal of faith in being successfully untraceable. Cryptography made this possible. PGP – "Pretty Good Privacy" – was one of the early and important tools, perhaps the first consumer-oriented cryptography. Another very important tool was the secure anonymous remailer (cf. Froomkin 1997: 129).

An anonymous remailer works as follows: Alice sends out an email destined for Bob which contains within it one or more layers. Each layer consists of an encrypted message, which I will call the payload, and unencrypted delivery instructions, making the entire message something like a sealed paper letter with an address written on the front. Although destined for Bob, Alice addresses the message to a remailer operator. The remailer operator strips off the headers of Alice's email – the part that identified it as coming from her – and forwards the payload message as directed. Alice could direct that the payload go to a second remailer, who would decrypt the payload only to find in it another layer of address and (to him) unreadable payload. By chaining the message in this manner through two or more remailers, Alice could ensure that before the message reached Bob its origins would be thoroughly obfuscated. What is more, if Alice and Bob used encryption to exchange messages, then none of the remailer operators would ever know what Alice was saying. Even if Bob was not so sophisticated, only the last remailer in the chain would be capable of reading the cleartext, and that person would have no way of finding out who originally sent the message unless every remailer in the chain kept logs and cooperated in unraveling the message's path.

Sending messages this way was never easy, and would be harder today because there are fewer reliable remailers. Remailers ran into two serious problems. The first is that spammers abused the remailer network. Strangely, a small amount of spam is a good thing for the remailer network because the spammers can be relied on to create a certain volume of traffic and this makes it harder for any observer to trace the genuine messages as they move through the network (ib.). But in short order the volume of spam increased to the point that so much spam went through the network as to first burden it and then choke many of the remailers entirely (Canter 2003).

Worse, the remailers faced a serious legal problem. The end point in any chain of remailers – the exit node – carries legal risk for misuse of the network. If, for example, your computer was used to send a death threat to the US President, ignorance of the message's content was not a comforting defense, and certainly was no shield against an investigation. To say that the entire process was automated did not necessarily provide a sufficient defense either.[2] As governments and police departments became more technologically savvy, the email operators increasingly decided it was just too unsafe to run a remailer, or at least to run an exit node. As fewer and fewer remailers were willing to be exits, the ones that persisted became overwhelmed with all the

2 Notably, the protections of the CDA against civil liability for third-party postings do not apply to criminal law. 47 U.S.C. §230(e)(1).

spam that sought release into the greater Internet, thus accelerating the network's death spiral.

Almost all these anonymity systems depended on some kind of cryptography. Western governments, and in particular the U.S. government, worked very hard to slow the spread of consumer cryptography. Governments were basically able to restrict the spread of cryptography, originally through export control (Froomkin 1996: 15–75). By preventing standardization, they made it easier to maintain the wiretapping and interception capabilities of both national security services and ordinary law enforcement. For many years this project of prevention was successful, and consumer cryptography was rare; indeed, only specialists used it – the presence of strongly encrypted traffic was sufficiently unusual to raise the possibility that observers might use it as a signal that one had something to hide, drawing extra attention from the authorities.

All these things undermine access to anonymity (in the strong sense). We can divide the history of Internet communications into three periods when using anonymity as a yardstick. In the first period, as noted above, anonymity was easy if you knew what you were doing, but it was not available easily to the consumer. This period ended when the remailers died off and strong anonymity was reduced to what I would call a 'safety valve' technology. That is, although it was no longer as easy for the technologically adept to achieve strong anonymity, it was still technically feasible. That mattered: if you were, for example, a sufficiently motivated dissident organization – you could be anonymous if you had to be. But for most people anonymity was either not available at all or it was foreseeably traceable: it was predictable that governments or others could trace the author without extraordinary effort. Today, anonymity online is not even a safety valve: it is increasingly difficult, sometimes impossible, for everyone.

2 The source of the demise of anonymity

Today the outlook for online anonymity is much worse than it has ever been before, and there is, I fear, little hope for improvement. The sources of this change extend well beyond the government surveillance revealed in the Snowden revelations (Strohm et al. 2014; Greenwald 2013; Kelion 2013; ib. 2014; Gellman 2013; Ball 2014; cf. Ball et al. 2013). There are in fact five reasons for this development. First, there is a widespread ideology that says anonymity is a bad thing in itself and ought not to be allowed. A second source is the profit motive. It turns out that there is quite a lot of profit in not having anonymity. The next two things are technological. Both governments and the private sector built a series of tools that greatly improve their abilities to track users online. These technologies are synergistic with other tools that enhance the linkages between online and off-line tracking. Off-line tracking is already prevalent and still growing, which means that it is ever harder to be anonymous online. Where in the past we observed the online world intruding into, and altering, the real world, now we

see the reverse: the real world invades and affects the online. And last – because it was somewhat late to the party – is the law, both at the national and the supra-national level.

Powerful motives animate the effort to make anonymity traceable, or indeed impossible. The most visible of these motives is the felt needs of national security, an argument pressed with increasing energy since 9/11. This concern over security is fueled by the fear that bad actors are using (or will use) this technology to inspire others to do harmful things, and that it empowers communications among terrorists who will be working in secret. The spies and policeman, it is claimed, will be left defenseless.

It is easy to imagine the anonymity issue from the point of view of a government official. A reasonable official might well believe that if she refrained from deploying some available technology of surveillance, and then something terrible happened, everybody would blame her. This scenario is what many officials actually believe, and this belief therefore pushes the people in government towards ever-increasing surveillance (Baker 2010: 5, 72).

This tendency in government, to push for technologies of identification in fear of not being able to catch someone doing something bad, is a truly global phenomenon. It is found in the UK (c.f. UK Identity Cards Act 2006: c.15), Australia (Parliament of Australia 2015), and in Pakistan (Computer Science and Telecommunications Board 1996: 438). Iran recently announced mandatory identification for everybody who goes online – as soon as they can figure out how to do it (The Economic Times 2011; Sharma 2011). India has been monitoring electronic communications for many years. It has a very elaborate and expensive centralized monitoring system, aimed at the Internet, called the "Lawful Intercept and Monitoring System" (Singh 2013).

The Indian story is instructive as it shows some of the limits of the law as a tool for combatting even government surveillance. Indian courts said that the Indian government needed a warrant to access email and telephonic communications (Prakash 2013). As a condition of receiving a license to operate, all internet service providers (ISPs), and all telecom providers, are required to provide the Indian government direct access to all communications passing through their systems, and must do so without a warrant (Freedom House 2014). India also requires that the carriers make sure that only weak encryption is used with their equipment in order to ensure that everything they carry is very easily accessible to authorities (Verma 2015). Furthermore, privacy safeguards built into the "Lawful Intercept and Monitoring System" appear to be ignored (Singh 2013).

Some other countries are not spending quite as much money as India and are not quite as strong in their licensing requirements, but they are enforcing identification nonetheless. In many countries, a major method of access to Internet is through cyber cafés. To destroy anonymity, governments pass a law that says cyber cafés must ask for ID and keep a log of who is using which machine at what time. This creates a record

that the government can always access if it traces a message's IP number to a particular machine in a cybercafé, thus allowing it to link the message to a person.

In the United States, the view that anonymity is dangerous is associated with Justice Scalia of our Supreme Court, who wrote in a 1995 dissent that anonymity is generally dishonorable because "[i]t facilitates wrong by eliminating accountability, which is ordinarily the very purpose of the anonymity" (McIntyre 1994: 514 U.S. 334, 385). To create legal protection for anonymous communication absent a reason to expect "threats, harassment, or reprisals," he argued, "seems to me a distortion of the past that will lead to a coarsening of the future" (ib.: 334, 385). However, in the *McIntyre* case as well as in other recent decisions (cf. Watchower Bible 2001: 536 U.S. 150, 166), the Supreme Court has found that there is a right to anonymous speech in the US Constitution. That means US citizens and permanent residents are protected against US laws criminalizing or otherwise preventing anonymous speech. We are not protected against government actions that have the side effect of making anonymous speech impossible nor against anonymity-blocking actions in the private sector. Thus, although we have a constitutional right, it turns out not to be as meaningful as it probably sounds.

In other countries, such as the UK, identification is incentivized by liability rules. The UK Defamation Act 2013 amended the UK's libel laws to stop the problem of people going to the UK and suing for Internet speech that originated somewhere else. The new Act provides that it is a defense for a website operator to show that she was not the author of the challenged material, but only if the identity of the real author is readily apparent, or if the website operator has complied with regulations concerning how to respond to notices of alleged defamation (Defamation Act, 2013: c. 26 U.K.). This puts pressure on the website owner. If the website owner cannot identify the speaker, then she has 48 hours following notice of the libel claim to take down the post or the speech is treated as her own (ib.). The United States, of course, is at the other extreme. Section 230 of the Communications Decency Act immunizes the owner of the website for almost all hosted third party speech unless the plaintiff can show that the website owner said it himself. Most other countries do not take that view, and a website operator is responsible for policing whatever speech appears there.

The United States, and other countries, also adhere to another important ideological view that has worked against anonymity, an ideology of responsibility that is rooted in feminist ideas. Numbers of feminists, including one of my colleagues (Franks 2011: 224–261; ib. 2012: 655–704), think it is tremendously important to punish people harming women online. Feminists point to “revenge porn,” the posting of nude pictures of ex-girlfriends as a form of oppression that they want to eliminate, and have ignited a movement sweeping the US to require website operators either to identify the source of the picture or be held responsible for it themselves (Peterson 2015). The consequences for anonymity are obvious. If you are creating a website capable of hosting photographs posted by others, you cannot know in advance what sort of photo-

graphs will be posted there. Therefore, under this regime, you have to be able to find everybody who uses your website for fear they might post one of these pictures.

3 The technological drivers of the demise of anonymity

Other technologies neither give people notice nor a choice as to how they will be identified. “Trusted computing” is a set of technologies designed to serve the needs of digital rights management (DRM). The theory is that users cannot be trusted, and hence content providers need to know exactly who is accessing their content. Manufacturers put an identification chip into a device, and design the operating system to allow third parties to see the ID, but prevent the device’s owner from masking the ID (Woodford 2004: 253–280). Content providers love this, as it permits them to append a unique identifier to every licensed download that encodes the user’s ID without the machine owner’s knowledge. That way, if a digital copy of the content should turn up on somebody else’s machine, the rights-owners will know who to sue.

The protection of intellectual property rights is a globally accepted norm. The problem with ‘trusted computing’, however, is that the same technology that enables strong DRM can easily be accessed by other applications designed to identify the user. The fundamental design feature of ‘trusted computing’ is that the user can have no control over it, or at most very limited control over it (Anderson 2011).

The profit motive obviously drives DRM; it also drives other attempts to ensure that customers are identified. Recently, MasterCard made a submission to Australian regulators in a formal procedure in which the Australian government was trying to decide how and whether to regulate BitCoin, a somewhat anonymous payment technology (Hajdarbegovic 2014). MasterCard made a very strong submission to the Australian regulator which said, we are regulated and have to know our customers and therefore no one else should be allowed to provide anonymous payment services. "[A]ll participants in the payments system that provide similar services to consumers should be regulated in the same way to achieve a level playing field for all" (ib.). And that level playing field should involve maximal consumer transparency, thus "consumer protection, anti-money laundering (AML), counter-terrorist financing (CTF) and stability should be the cornerstones of any regulation of electronic payments, including digital currencies"(ib.).

MasterCard’s sole proposal was that nobody should have privacy by law, and no one should be allowed to offer it. That is a disturbing indicator suggesting that the desire to protect the profit and business models of companies that heavily invested in identification technology has set off a race to the bottom in which regulations will be invoked to limit competing privacy-enhanced products. One would have much preferred to see a so-called ‘struggle to the top’ in which firms competed to provide privacy-enhanced products.

Indeed, identifying technologies are already widespread. Some are operated at the ISP level, some are in telephones, and some operate at the legal level. You cannot talk today about any online issue without talking about telephones. Predictions are that telephones will be eclipsing PCs very shortly as a means to get online (Standage 2013). Telephones come configured as a privacy wasteland. Because the engineering of the cell phone network is entirely about identifying the user, your phone is constantly providing data about you and that information is used to identify you and link to offline databases.

In the United States, if a person walks into a store it is perfectly legal for the store to detect the wi-fi signal that their phone emits as it tries to connect to a network. That signal has a unique identifier. It permits the store to track customers as they move around the store, and it links to that record if the customer ever revisits the store. Linking the customer to a past purchase may make it possible to send the customer advertisements or discount coupons.

From a strictly pocketbook point of view, this might be a good thing for consumers as they get offered a discount. Indeed, this is the method by which most phone-based technology, most apps, convince people not to be too concerned. The surveillance is sold to consumers as empowering, in the sense that it makes possible the functionality of the app. But one need only look at a modern smart phone to see the great breadth of the permissions which installed apps require in order to function. It is common on installation to see a great mismatch between the permissions that the app asks for and what it actually needs to function. On my phone, apps commonly demand to have access to my location, even though they are not a name- or location-based service. The choice is to take it or leave it. And we take it. And thus there is no privacy if you use your phone.

4 Political drivers of the demise of anonymity

But it gets worse. If you are using a cell phone, or an old fashioned telephone, or a computer, to access the internet, there is probably one – if not several – government-sponsored data collection devices monitoring your communication. This is one of the things we learned from Edward Snowden, and even before him, where people had stumbled upon these strange rooms in ISPs company where there were far more computers, recorders and wires than had any right to be there (Hepting 2008; In re NSA 2008). We know from statistics that came out in the Snowden revelations that as of May 2012, US security services and their allies had collected technical information on about 70 percent of the cell phone networks in the world. They had data on 701 out of 985 known cell phone networks (Ferranti 2014). As for the physical undersea cables that move communications transnationally, it is believed that every one of those cables has a tap attached to it (Khazan 2013), which is why some countries now want to

build their own undersea cables (Scola 2014), which I interpret, perhaps cynically, to mean they want to own the taps.

The information architectures we use route our information via strange places, such as "the cloud", further undermining our privacy. One could encrypt all one's data so that tapping the cloud would be less useful, but few people do that. And even encryption has become an uncertain friend. This is another thing we have learned from the Snowden revelations: that the US National Security Administration (NSA) has worked quite hard in two known cases – and, we fear, in others that we don't know about – to weaken encryption standards in a way which makes them easier to break (Arthur 2013). These decryption projects still take some computation, but much less than would be required if the algorithms had not been engineered to carry hidden defects. The tools meant to protect us and protect our information are no longer reliable. It is no longer reasonable to have faith in even those international standard-making processes that had been the gold standard for reliable cryptography, because very subtle changes were introduced into these processes via government employees supposedly working independently in a private capacity (The Economist 2013). As investigators and analysts discover these weaknesses, they propose new and one hopes better standards. But that still leaves a large unpatched installed base which can take a long time to catch up to the new versions, if indeed they are capable of being patched and the new versions are compatible.

In contrast, sometimes the things that would identify us are put out in the open for everyone to see, but that can provoke resistance. An example comes from the Domain Name System (DNS), which uses what are called IP numbers. IPv4 is the old system and the address space is nearly used up. It has only 2^{32} numbers, or about four billion possible numbers, which is fewer than the number of people on the planet. The internet is in the process of moving to IPv6, which offers us 2^{128} numbers, which is about 340 decillion, enough in theory to give every person on earth several octillions of IP numbers and still have plenty left over (Goldman 2012). The original IPv6 specification for email required that every email packet would include the MAC number in the header, uniquely identifying the device that sent the packet. As a result, every packet sent would be immediately traceable to the device that sent it. This created such a furor that the Internet Engineering Task Force (IETF) came out with an alternate, if optional, standard which includes privacy enhancements (Narten et al. 2007).

It remains possible that by going to the public library, or to the university, or to the cyber café, one can avoid being linked to a message – so long one does not have to show ID to use the public computer, and so long as there is no camera there watching who is using the equipment. But today, both government and private security cameras are ubiquitous indoors and out, making it nearly impossible to be anonymous offline.

5 Self-Surveillance as a driver of the demise of anonymity

And then there is self-surveillance. Twitter, Instagram, Facebook, all offer opportunities to sabotage one's own privacy. Using a decent camera and increasingly accurate of facial recognition software, we have now gotten to a point where if you have a Facebook account, there is a 75% chance that a computer can match a picture taken of you to your Facebook account in less than 2 seconds (Acquisti et al. 2014). Not having a Facebook account is little protection. If somebody else on Facebook took a picture of you and tagged it, it is the same as doing it yourself.

The public and private data collectors are almost merged outside of the EU, practically the only place where there are significant limits on data re-use. In the rest of the world, and especially in the US, they are all sharing with each other. In the United States all sorts of government information, including some disclosures required to obtain certain permits, is for sale. Meanwhile the marketers are selling their data to the government, which uses it for ID authentication among other things. In the name of national security, the US is also building ever-larger databases, which brings us to the world of big data. The internet of things means that we will have all sorts of devices that talk to each other on the internet, so your refrigerator will know when you are home, it will know what you are eating and it will tell your insurance company about your diet. Your life insurance rates will be adjusted according to whether you ingest too much cholesterol.

6 Law and the demise of anonymity

So where does law fit into all this? The common-law nations have approached the Internet with a three-step procedure. The first step has been to look at some of the activity on the internet, like email and electronic documents, and to try to categorize those things, or those activities, as akin to something familiar, both because this is how lawyers think and because it is less work.

When that approach failed to cover all the new phenomena, or just could not be made to fit because that internet thing was too different, the next step was to create new categories or in some cases to create new institutions like ICANN.

Meanwhile, there was a third step: a bold attempt to turn back the clock. New channels of speech, new channels of commerce, and of course new methods of copying and sharing content, each discomfited and disrupted established practices or threatened profitable business models belonging to powerful institutions. In the case of law enforcement, common investigative techniques seemed to be at risk. These institutions sought to prohibit the new things that endangered the established order. For a long time the best example of this was the campaign by Big Copyright for DRM. Copyright interests carried out a successful campaign to enact new copyright restrictions, to protect against digital technologies, and to get the law to make copyright violation an increasingly serious offense (Digital Millennium Act 1998). The *loi Hadopi*

was an example of this in France (Dejean et al. 2010), until it was struck down (Conseil Constitutionnel 2009), although even then copyright interests secured passage of a corrective, known as "Hadopi 2"(Loi 2009-1311 du 28 octobre 2009).

7 A goldfish bowl society

The push against anonymity has had even greater success than the push against copyright violations. Copyright violations are still ongoing; we need only consider the cases of torrent sites, or the notorious Pirate Bay (Cook 2014), to see that. But for those seeking to speak anonymously, there really is no place to go. There is more identification and more surveillance online – especially through the linking of the online and offline – than I think has ever before existed in human history. We have radically overcompensated. The Internet plus cellphones, plus sensors, equals basically a goldfish bowl society, and we are the goldfish.

The state can use this privacy-compromising technology in all kinds of overt and subtle ways. The subtle ones may be worse than the overt ones because people become nervous about doing things, the so-called chilling effect. We have seen examples of this in New York City where the police created a Facial Recognition Unit to identify suspects – and demonstrators – via Instagram and Facebook (Weis 2013). Ukraine had a demonstration recently, and the government set up a fake cell tower – stingray is the name of the technology – collecting information on cellphones held by the people in the area. It then sent text messages, "Hello, we are the police. Your position has been reported and being at an illegal demonstration, just thought you'd like to know we know" (Merchant 2014). This is a way of keeping people home. It works.

In the West, we have used the law to enlist key intermediaries as our identity collectors. Here the template was the banking system, which has for many years been subject to "know your customer" rules in which banks and other financial intermediaries must collect information about people before accepting their deposits and processing their payments. ISPs, the choke points in the internet ecology, were next. There has been a gradual effort to get ISPs to collect as much information about their customers, and their customer's communications, as the cellphone company gathers. As is well known, U.S. law has special Constitutional protections for speech (US Constitution Amendment I), and supposedly against government searches (US Constitution Amendment IV). It is worth pointing out when you mix the adoption of encryption with the legal protection of anonymous speech, it creates a major tension that U.S. law has not yet resolved. The legal problem exists because every packet of encrypted digitized data looks alike from the outside. If the legal system imagines that there might be any class of disfavored and thus unprotected speech, whether it is pirated movies, terrorist conspiracies, obscenity, or revenge porn, widespread encryption undermines the ability to control the spread of that content. And if a key element of that control involves finding the party responsible for the bad speech, cryptography-based anonymity tech-

nology becomes a major problem. The technological measures necessary to be able to pierce anonymity must be applied to every packet on the network or it is meaningless. Either we allow as much anonymity as users want, or we allow none at all.

8 Safeguarding anonymity

Can anonymity online be saved? The question currently makes sense only for computers, because for cellphones the game is fully lost. To protect identities in the cell phone world would take a whole new hardware, a whole new architecture, and given the size and value of the installed base and the power of incumbent carriers, one has to ask if this is even possible. Even for the world wide web, reclaiming space for real anonymity would take many changes. It would take the full encryption of the web transport mechanisms (Casaretto 2014).[3] It would require the repeal of all laws that enable digital inspections, in which the government can look inside the packet to tell whether it is a bad packet or a good packet. It would require control of ongoing efforts of national security agencies to collect and store all the metadata information that describes where the packet came from and where it is going. And, crucially, it requires standards we can trust. This is the biggest barrier, because that trust requires relying on a mathematical expertise that only a small number of people have.

To make email anonymity real, we would need many things we do not have at present. To start, we would need a widely shared encryption tool; in addition we would need an infrastructure of remailers, a thing that is quite unlikely for all of the reasons mentioned above, notably the spam and the legal risks.

More generally we would need a deeper and broader understanding of what privacy means and why it matters. Because ultimately the anonymity problem is converging with the big data problem: the more that governments and firms place sensors everywhere and collect masses of information about everyone online and off and then use it to build profiles about us, the less there is any place to hide. Thus, we must now ask whether there are the legal or social solutions to the problem of these profiles.

9 Data retention

It is true that on the data retention question alone we have relatively good results, especially in the EU. There was a major decision by the European Union Court of Justice in April 2014 annulling the proposed data retention rules (Digital Rights Ireland 2014), and it did so on the basis of the European Convention of Human Rights, and on case law from the European Court of Human Rights, which importantly opens the doors to linking these two sets of law. Henceforth, in the EU data retention cannot be general but must be necessary and proportionate. Data collected for one purpose can only be re-used for law enforcement if there is a link to a specific threat to public safe-

3 Although growing quickly, current https traffic remains a small fraction of total web traffic, being only 3.8% in North America in 2014, 6.1% in Europe, and 10.37% in Latin America.

ty and the risk of stigmatization stemming from inclusion in the police data basis is limited. Either before this decision, or as a result of it, the national courts in many countries of the EU have struck down data retention. Many more countries have challenges pending.

But outside Europe it is a different story. In Australia, data retention is proceeding apace. Indeed outside of Europe and the U.S. we don't have at the moment mandatory data retention, we just have an open door. A number of Latin American countries are discussing data retention laws. To the extent that some people look to the Inter-American Convention on Human Rights (Inter-American Commission on Human Rights 1969), there is a little relevant case law. And then in Asia, and especially in China, there tends to be even less scope for anonymity.

In the United States as a formal matter, we do not have a data retention mandate at present. But there is a terribly fictional element to that claim as we have learned that our government is already gathering and storing massive amounts of communications traffic (Ball 2014).

10 Some unintended consequences of the Snowden revelations

This brings us to yet another perversity in privacy and security policy. In addition to all their positive effects, the Snowden revelations may have two other unanticipated negative effects. Let me not be misunderstood; so far, the consequences have been positive. But we need to understand what all the consequences may be. One likely consequence is that a number of governments will now officially make legal what was previously done secretly. We are already seeing this in Ireland which is setting up a new system of surveillance in which ISPs and telephone companies can be required to provide data to the government and if they are unwilling there is a new secret court to make them – in effect creating a whole new judicial system (Lillington 2014). The second thing is that we now know that the NSA has been collecting data domestically on a large scale. This was a major secret, so much so that it greatly constrained the NSA's willingness to share data with civilian law enforcement authorities although it did not completely prevent it (Fakhoury 2013). The NSA apparently feared that information about its capabilities and activities might come out in court, and the NSA considered this knowledge to be a national secret of too high value to take that risk.

Now we find ourselves in a different place. We now have evidence that the NSA and its companion agencies in several other countries have been capturing communications and sharing them with each other (Corera 2013). As a result, it seems only logical that the NSA and other nations' security agencies too, will become much more willing to share the fruits of their communications acquisition with domestic law enforcement agencies. If and when this comes to pass, privacy actually might become weaker as a result of Snowden's exposure of these surveillance technologies.

11 The limited potential of International Human Rights law

Lawyers naturally wish to find solutions to social problems in the law. After all, if access to anonymity is so closely tied to the preservation of autonomy and personal privacy, and if this problem is indeed global in scope, that sounds as if it should be an international human rights problem. Can International Human Rights (IHR) law do the job here? Again, I have a rather pessimistic assessment. There is no real sign that IHR law provides the tools to address this problem, and if it could, the enforcement mechanisms outside the EU are notoriously weak. Although there is some basis in IHR law to seek protection for privacy, broadly defined, it is not the same as anonymity and indeed it is fairly clear in most of the relevant instruments that anonymity is something they wish to exclude from protection. Indeed, a rare clear discussion of the protection of anonymity in IHR law is found in the Council of Europe's Declaration of Freedom of Communication on the Internet of 2003 where it says on article 7, principle 7:

> In order to ensure protection against online surveillance and to enhance the free expression of information and ideas, member states should respect the will of users of the Internet not to disclose their identity. This does not prevent member states from taking measures and co-operating in order to trace those responsible for criminal acts, in accordance with national law, the Convention for the Protection of Human Rights and Fundamental Freedoms and other international agreements in the fields of justice and the police (Council of Europe, Committee of Ministers 2003).

So even there, in what is perhaps the high watermark for protection of anonymous speech in IHR law, we see major carve-outs and limitations.

But this is still more than we find in other instruments. Article 19 in the Universal Declaration in Human Rights provides that "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers" (UN 1948). Similar protections of communicative freedom appear in other important international agreements, for example Article 19 of the International Covenant on Civil and Political Rights (UN 1976), but in every case either implicitly or more commonly explicitly the relevant rights are hedged with the idea that *ordre publique* or something similar justifies finding the identity of the speaker – that it is important to ensure that communicative freedom is not used for crime. Thus the International Covenant on Civil and Political Rights provides for a number of important communicative freedoms and then qualifies them by saying that they "may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary" whether for the "respect of the rights or reputations of others" or "for the protection of national security or of public order, or public health or morals" (ib.; Grisby 2014).[4] Those are very broad categories.

4 On November 25, 2014, the third committee of the UN General Assembly adopted a resolution that calls on states to "respect and protect the right to privacy" in the digital age. Surveillance of digital communications "must be conducted on the basis of a legal framework". The final Report, however, removed text from an earlier draft that said surveillance needed to conform with principles of pro-

The EU idea is better, but only somewhat. The EU seems to believe that large amounts of personal data may be collected, but once the data are collected it is possible to impose limits on reuse. From my pessimistic perspective, proportionality means that the information is going to be available, waiting to be analyzed, waiting to be used, if a government body finds that there are sufficient grounds to do so. One is asked to trust the people holding the information, despite what we have learned from Snowden.

12 Conclusion and outlook

That trust approach is different from the appeal of anonymity in the strong sense. Anonymity is a safety valve technology when trust is absent or the future uncertain. In a world of increasing surveillance we have never needed that safety valve more than we do today. It provides a mechanism, one at present complex and not utterly reliable, from which we derive some hope of blocking the growth of profiling, and some hope of communicating without it necessarily being traced back to us – because otherwise everything can be traced back to us. Neither in domestic law nor in international law do we see a strong commitment to anonymous speech at a time when it is so much in need of protection. I think that Justice Scalia spoke for many people, particularly those in power, when he said he thought there was something fundamentally dishonorable about anonymous speech (McIntyre v. Ohio Elections Comm'n 1995).

Many governments simply do not trust their people and are afraid of honest speech because it might lead to something revolutionary. Others may not fear revolution but they fear crime, hate speech, or the theft of intellectual property. So the combination of these things means there is basically no constituency for anonymity at the international level nor at the government level other than a few NGOs – but they do not get to make national, much less international, law. Add in the bilateral and multilateral trade treaties that often create new protections for intellectual property, and recall that many of these protections will require identification in order to be effective. The bottom line is that anonymity online is not just in danger, but on life support.

The plight of online anonymity can no longer be seen as just a technical issue. It is political. The anonymity issue is an inextricably interconnected with technical issues for the standards for phones and for computers, for apps, for 'trusted technology', for intellectual property. It is connected to strong market-based incentives because there is money to be made from identification and profiling. Anonymity also suffers from its connection to very powerful imperatives and bureaucratic incentives in the name of national security.

The anonymity issue has merged into the online privacy issue, and the online privacy issue is merged into the offline privacy issue, and in fact has become just the privacy

portionality, legitimacy, and necessity—principles that are not [explictly] contained in the International Covenant on Civil and Political Rights (ICCPR) (ib.).

issue with no adjectives. The question therefore is really to what extent consumers and voters are going to decide they care about privacy. And the history so far suggests that the answer is that they care a little bit, not zero, but not enough to push against all the other forces deployed in this arena. I continue to believe that the lack of panic is primarily because most people do not truly understand how much they are being surveilled – because surveillance, especially online, remains mostly invisible. I think there is still hope; if we can make surveillance more visible, there is hope that enough people will get excited about the issue to matter. But this is only a hope and in no way a certainty.

In the process of offering anonymity as a response to surveillance, it will be important to deal with the very legitimate, and if not legitimate certainly honestly and deeply felt, concerns of people who think that there is something wrong with anonymity, that it encourages people to be bad. Part of that solution will be to devise other ways to deal with the bad things people do online. So, for example, if we had a consensus for ridicule and social ostracism of people who are the sources of revenge porn (most of whom will be known to the victims), and also for those who enable them, this might help prevent it and reduce the calls for ubiquitous deployment of identification technology.

Although not all is lost yet, realistically one must conclude that the prognosis for strong anonymity is fairly grim. I invite you to prepare to enjoy swimming in the digital goldfish bowl.

Bibliography

Acquisti, Allessandro / Gross, Ralph / Stutzman, Fred (2014): Face Recognition and Privacy in the Age of Augmented Reality, in: Journal of Privacy and Confidentiality 6:2, 1, http://repository.cmu.edu/jpc/vol6/iss2/1/ (24.07.2015).

Anderson, Ross (2011): Trusted Computing 2.0, in: Light Blue Touchpaper), https://www.lightbluetouchpaper.org/2011/09/20/trusted-computing-2-0/ (26.06.2015).

Arthur, Charles (2013): Academics criticize NSA and GCHQ for weakening online encryption, http://www.theguardian.com/technology/2013/sep/16/nsa-gchq-undermine-internet-security (22.06.2015).

Baker, Stewart A. (2010): Skating on Stilts, Hoover Institution Press: Stanford, CA.

Ball, James / Ackerman, Spencer (2013): NSA loophole allows warrantless search for US citizens' emails and phone calls, http://www.theguardian.com/world/2013/aug/09/nsa-loophole-warrantless-searches-email-calls (15.07.2015).

Ball, James (2014): NSA collects millions of text messages daily in 'untargeted' global sweep, http://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep (15.07.2015).

Canter, Sheryl (2003): Hiding Your Identity, PC Magazine, http://www.pcmag.com/article2/0,2817,1230752,00.asp (14.07.2015).

Casaretto, John (2014): The Internet strikes back, Global encrypted SSL traffic booms, http://siliconangle.com/blog/2014/05/20/the-internet-strikes-back-global-encrypted-ssl-traffic-booms/ (26.06.2015).

Computer Science and Telecommunications Board (1996): Cryptography's Role in Securing the Information Society, National Academy Press: Washington, D.C.

Conseil Constitutionnel (2009): Décision n° 2009-580 DC du 10 juin 2009, http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/2009/decisions-par-date/2009/2009-580-dc/decision-n-2009-580-dc-du-10-juin-2009.42666.html (24.07.2015).

Cook, James (2014): The Pirate Bay Speaks Out About the Police Raid That Shut It Down: 'We Couldn't Care Less', http://www.businessinsider.com/the-pirate-bay-speaks-out-about-the-police-raid-we-couldnt-care-less-2014-12 (22.06.2015).

Corera, Gordon (2013): Spying Scandal: Will the 'five eyes' club open up?, http://www.bbc.com/news/world-europe-24715168 (22.06.2015).

Council of Europe, Committee of Ministers (2003): Declaration on Freedom of Communication on the Internet, article 7, principle7, https://wcd.coe.int/ViewDoc.jsp?id=37031 (24.07.2015).

Defamation Act, (2013): chapter 26 (U.K.), http://www.legislation.gov.uk/ukpga/2013/26/contents/enacted (15.07.2015).

Dejean, Sylvain / Pénard Thierry / Suire, Raphaël (2010): Une première évaluation des effets de la loi Hadopi sur les pratiques des Internautes français, http://www.marsouin.org/IMG/pdf/NoteHadopix.pdf (17.08.2015).

DeLong, J.B. / Froomkin, A.M. (2000): Speculative Microeconomics for Tomorrow's Economy, in: Internet Publishing and Beyond: The Economics of Digital Information and Intellectual Property, http://www.law.miami.edu/~froomkin/articles/spec.htm (14.07. 2015).

Digital Millennium Act (1998): 17 U.S.C. §512, 1201 to 1205, 1301 to 1332, 28 U.S.C. §4001.

Digital Rights Ireland Ltd v Minister for Communication (2014): Joined Cases C-293/12 & C-594/12, 11-16 (Ct. Justice E.U. Apr. 8, 2014), http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=161279 (26.06.2015).

Fakhoury, Hanni (2013): EFF, DEA and NSA Team Up to Share Intelligence, Leading to Secret Use of Surveillance in Ordinary Investigations, https://www.eff.org/deeplinks/2013/08/dea-and-nsa-team-intelligence-laundering (24.07.2015).

Ferranti, Marc (2014): NSA Spy Program Targets Mobile Networks Worldwide, http://www.pcworld.com/article/2856352/nsa-spy-program-targets-mobile-networks-worldwide.html (22.06.2015).

Franks, Marry Anne (2011): Unwilling Avatars: Idealism and Discrimination in Cyberspace, in: Columbia Journal of Gender and Law 20: 224–261.

Freedom House (2014): India, Freedom on the Net, https://freedomhouse.org/report/freedom-net/2014/india (15.07.2015).

Franks, Marry Anne (2012): Sexual Harassment 2.0, in: Maryland Law Review 71: 655–704.

Froomkin, A. Michael (1995): Anonymity and Its Enmities, in: Journal of Online Law Article 4, http://groups.csail.mit.edu/mac/classes/6.805/articles/anonymity/froomkin.html (14.07.2015).

Froomkin, A. Michael (1996): It Came From Planet Clipper, in University of Chicago Law Forum.

Froomkin, A. Michael (1997): The Internet As A Source Of Regulatory Arbitage, in: Kahin, Brian / Nesson, Charles (eds.): Borders In Cyberspace, MIT Press: Cambridge, Mass.

Gellman, Barton (2013): NSA broke privacy rules thousands of times per year, audit finds, http://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html (15.07.2015).

Goldman, David (2012): The Internet Now has 340 Trillion Trillion Trillion Addresses, http://money.cnn.com/2012/06/06/technology/ipv6/ (22.06.2015).

Greenwald, Glenn (2013): NSA collecting phone records of millions of Verizon customers daily, http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order (15.07.2015).

Grisby, Alex (2014): UN Committee Adopts Resolution on Right to Privacy in the Digital Age, in: Council on Foreign Relations: Net Politics, http://blogs.cfr.org/cyber/2014/12/01/un-committee-adopts-resolution-on-right-to-privacy-in-the-digital-age/ (26.06.2015).

Hajdarbegovic, Nermin (2014): MasterCard Seeks 'Level Playing Field' for Bitcoin Regulation, http://www.coindesk.com/mastercard-seeks-level-playing-field-bitcoin-regulation/ (22.06.2015).

Hepting v. AT&T, 539 F.3d 1157 (9th Cir. 2008).

In re National Security Agency Telecommunications Records Litigation, 564 F. Supp.2d 1109 (N.D.Cal. 2008).

Inter-American Commission on Human Rights (1969): http://www.cidh.oas.org/basicos/english/basic3.american%20convention.htm (26.06.2015).
Khazan, Olga (2013): The Creepy, Long-Standing Practice of Undersea Cable Tapping, http://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/ (16.07.2015).
Kelion, Leo 2013: Q&A: NSA's Prism internet surveillance scheme, http://www.bbc.com/news/technology-23027764 (15.07.2015).
Kelion, Leo (2014): Edward Snowden: Leaks that exposed US spy programme, http://www.bbc.com/news/world-us-canada-23123964 (15.07.2015).
Legal Information Institute (n.y.): 47 U.S. Code § 230 - Protection for private blocking and screening of offensive material, https://www.law.cornell.edu/uscode/text/47/230 (15.07.2015).
Lillington, Karlin (2014): Surveillance by a Government-sponsored secret system, The Irish Times, http://www.irishtimes.com/business/technology/surveillance-by-a-government-sponsored-secret-system-1.2033443 (26.06.2015).
Loi 2009-1311 du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur internet, http://legifrance.gouv.fr/eli/loi/2009/10/28/JUSX0913484L/jo/texte (26.06.2015).
McIntyre, Joseph (1994): Certiorari to the Supreme Court of Ohio No. 93-986. Argued October 12, 1994-Decided April 19, https://supreme.justia.com/cases/federal/us/514/334/case.html (15.07.2015).
McIntyre v. Ohio Elections Comm'n (1995): 514 U.S. at 385 (Scalia, J. dissenting), https://supreme.justia.com/cases/federal/us/514/334/case.html (24.07.2015).
Merchant, Brian (2014): Maybe the Most Orwellian Text Message a Government's Ever Sent, Motherboard, http://motherboard.vice.com/en_ca/blog/maybe-the-most-orwellian-text-message-ever-sent (26.06.2015).
Narten, Thomas / Draves, Rich / Krishnan, Subramanian (2007): Privacy Extensions for Stateless Address Autoconfiguration in IPv6, RFC 4941, http://www.ietf.org/rfc/rfc4941.txt (26.06.2015).
Parliament of Australia (2015): Telecommunications (Interception and Access) Amendment (Data Retention) Bill, http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r5375 (15.07.2015).
Peterson, Andrea (2015): Activists in the war against revenge porn are finally seeing results, in: The Washington Post, http://www.washingtonpost.com/blogs/the-switch/wp/2015/02/20/activists-in-the-war-against-revenge-porn-are-finally-seeing-results/ (26.06.2015).
Prakash, Pranesh (2013): How Surveillance Works in India, in: The New York Times, http://india.blogs.nytimes.com/2013/07/10/how-surveillance-works-in-india/?_r=1 (15.07.2015).
Scola, Nancy (2014): Brazil Begins Laying Its Own Internet Cables To Avoid U.S. Surveillance, https://www.washingtonpost.com/news/the-switch/wp/2014/11/03/brazil-begins-laying-its-own-internet-cables-to-avoid-u-s-surveillance/ (22.06.2015).
Singh, Shalini (2013): Govt. violates piracy safeguards to secretly monitor Internet traffic, in: The Hindu, http://www.thehindu.com/news/national/govt-violates-privacy-safeguards-to-secretly-monitor-internet-traffic/article5107682.ece?homepage=true, (26.06.2015).
Sharma, Amol (2011): RIM Facility Helps India in Surveillance Efforts, in: Wall Street Journal, http://online.wsj.com/article/SB10001424052970204505304577001592335138870.html (15.07.2015).
Standage, Tom (2013): Live and Unplugged, http://www.economist.com/news/21566417-2013-internet-will-become-mostly-mobile-medium-who-will-be-winners-and-losers-live-and (22.06.2015).
Strohm, Chris / Wilber, Del Quentin (2014): Pentagon Says Snowden Took Most U.S. Secrets Ever, Bloomberg Business, http://www.bloomberg.com/news/articles/2014-01-09/pentagon-finds-snowden-took-1-7-million-files-rogers-says (15.07.2015).
The Economic Times (2011): RIM gives India access to Messenger services, http://articles.economictimes.indiatimes.com/2011-01-14/news/28430015_1_security-architecture-corporate-email-blackberry-enterprise-server (15.07.2015).
The economist (2013): Cracked Credibility, http://www.economist.com/news/international/21586296-be-safe-internet-needs-reliable-encryption-standards-software-and (22.06.2015).
UK Identity Cards Act (2006): chapter 15, http://www.legislation.gov.uk/ukpga/2006/15/pdfs/ukpga_20060015_en.pdf (15.07.2015).

UN (1948): The Universal Declaration of Human Rights, Article 19.
UN (1976): International Covenant on Civil and Political Rights, Article 19.
US Constitution Amendment I, http://www.usconstitution.net/xconst_Am1.html (24.07.2015).
US Constitution Amendment IV, http://www.usconstitution.net/xconst_Am4.html (24.07.2015).
Verma, Vivek Kumar (2015): Digital Encryption Laws in India, https://indiancaselaws.wordpress.com/2015/02/10/digital-encryption-laws-in-india/ (26.06.2015).
Watchower Bible & Tract Society of New York, Inc., et al. v. Village of Stratton et al. (2001): Certiorari to the United States Court of Appeals for the Sixth Circuit No. 00-1737. Argued February 26, 2002-Decided June 17, 2002, https://supreme.justia.com/cases/federal/us/536/150/case.html (15.07.2015).
Weis, Murray (2013): High-Tech NYPD Unit Tracks Criminals Through Facebook and Instagram Photos, http://www.dnainfo.com/new-york/20130325/new-york-city/high-tech-nypd-unit-tracks-criminals-through-facebook-instragram-photos (27.06.2015).
Woodford, Chad (2004): Trusted Computing or Big Brother? Putting the Rights Back in Digital Rights Management, in: University of Colorado Law Review 75, 1253–1317.

Author

Prof. A. Michael Froomkin
Laurie Silvers & Mitchell Rubenstein Distinguished Professor of Law
University of Miami
School of Law
1311 Miller Drive, Coral Gables, FL 33146
froomkin@law.miami.edu

DOI: 10.11588/josar.2015.0.23480

The **Journal of Self-Regulation and Regulation** is an open-access peer-reviewed journal serving as a potential outlet for edge-cutting interdisciplinary research on regulatory processes in individuals and organizations. It is published by the research council of Field of Focus 4 (FoF4) of Heidelberg University. The research council stimulates and coordinates interdisciplinary activities in research and teaching on self-regulation and regulation as part of the university's institutional strategy "Heidelberg: Realising the Potential of a Comprehensive University", which is funded by the Federal Government as part of the excellence initiative.

The *Journal of Self-Regulation and Regulation* publishes two volumes per year, regular volumes containing selected articles on different topics as well as special issues. In addition, the reader will be informed about the diverse activities of FoF4, uniting scientists of the faculty of behavioural and cultural studies, the faculty of social sciences and economics, as well as the faculty of law.

Imprint

Journal of Self-Regulation and Regulation Volume 01 (2015)

Research Council of Field of Focus 4, Heidelberg University
Forum Self-Regulation and Regulation
Hauptstr. 47–51
69117 Heidelberg, Germany

Fon: +49 (0)6221 / 54 – 7122
E-mail: fof4@psychologie.uni-heidelberg.de
Internet: https://www.uni-heidelberg.de/fof4

Publisher: Research Council of Field of Focus 4, Heidelberg University
Spokesperson: Sabina Pauen, Department of Psychology
Guest Editors: Wolf J. Schünemann, Department of Political Science
Sebastian Harnisch, Department of Political Science
Editorial Team: Melanie Bräunche, Sabine Falke

You can download the volumes of the *Journal of Self-Regulation and Regulation* free of charge at:
http://journals.ub.uni-heidelberg.de/index.php/josar/index