So Much for Savages: Navajo 1, Government 0 in Final Moments of Play

Eben Moglen[*]
Columbia Law School

March 1999

Dame i gospodo, uvažene kolege, počastvovan sam vašim pozivom da prisustvujem ovom značajnom skupu. Danas ću govoriti o ograničenjina baziranim na ustavnim pravima regulacije naše komunikacije, od strane vlade, a u interesu signorsti. Ali na kraju, kao što ćete i vi sami shvatiti nemo puno toga da se kaže, samo na osnovu toga što je naćin komunikacije nov. Pre svega treba se rešiti pitanje jezika. After all, every act of linguistic communication occurs in a social context. And the single most important choice that we make when we communicate with one another is the choice of the language in which we do so.

What I might have done by continuing to make my remarks this afternoon in Serbo-Croatian could be construed, I suppose, as a cipher. If there are one or two people here who are native speakers of Serbo-Croatian, my remarks become a message addressed solely to them, apparently for the purpose of excluding everybody else. Or perhaps I have a confederate here this afternoon, with whom I conspire not to make fun of your North American monolinguism but to redistribute your property at gunpoint; in such an event then perchance my remarks were a cipher intended for the advancement of criminal activity. If there were two listeners here—each a

[*] Professor of Law & Legal History, Columbia Law School. A slightly different version of these remarks was presented at the NYU Law School on November 19, 1998. Thanks are primarily due to Philip Zimmerman, the author of PGP, for creating the current mess. I wish to express my appreciation to Yochai Benkler, for helpful conversation and insightful analysis; and to the National Security Agency, for being the source of much innocent, if expensive, amusement.

highly nationalistic member of the fraternity of South Slavs, now dividing their language along an imaginary border soaked in real blood—my remarks might have been taken as some form of ethnic aggression. It is, after all, the social context of our communications that determines meaning, and not something in the nature of the noises. Much argument about the First Amendment's relation to encryption regulation fails to take account of this basic point: What the choice of language means depends entirely upon the context of its use.

In the fall of 1993 I was representing Philip Zimmerman, the author of a computer program called Pretty Good Privacy, in connection with a criminal investigation by the United States. Phil's program was the first serious attempt to make sophisticated data encryption at the highest technical level freely available to users of all personal computers. Naturally, once you grasp the mindset that has dominated the rulers of the American Empire since the end of the Second World War, this was too dangerous not to be illegal. I was talking to John Markoff of The New York Times, who was taking an interest in these obscure events, and I said, "The right to speak PGP is the right to speak Navajo." I meet that statement from time to time now in email signatures and usenet posts; it seems to have become part of the Bartlett's Familiar Quotations of the crypto wars. I chose Navajo at that moment precisely because Navajo embodies the basic social uncertainty that results from linguistic diversity. The Na–Dené languages are collectively an isolate.[1] They bear, as one accident of the evolutionary descent of human language over time, no demonstrable relation to any other languages on Earth.

As it happens, speaking Navajo, throughout the lifetime of all living native speakers, has been an assertion of cultural self-determination. During the long process of the imperialization of the continent by the United States, speaking Navajo—and other languages in other pre-European families represented within our borders—has been the central means of maintaining a cultural tradition apart from, and often explicitly hostile to, the government exercising control over the territory.

But in one of history's little ironies it has also, from time to time, suited the United States Government to take advantage of Navajo as a cipher—a story with which, I imagine, some of you are familiar. Before electronic dig-

[1]The languages comprising the family are Navajo, Chipewyan, and Tlingit. The total population of native speakers is considerably less than 200,000, of whom all but 9,000 or so are speakers of Navajo. *See* DAVID CRYSTAL, THE CAMBRIDGE ENCYCLOPEDIA OF LANGUAGE, Appendix III (1987).

ital cryptography was developed, during the Second World War, the United States military used Navajo speakers as an encrypted form of radio communication in the Pacific theater of operations. What was in one context cultural self-determination and an assertion of a human right against the United States Government, was in another locale military-grade encryption. So there we find ourselves with the central, and regrettably mostly unaddressed, argument concerning all the encryption regulations with which you presently have been told there are no First Amendment problems.

May the United States government require English to be spoken in the telecommunications network of the United States? We could reduce the federal budget substantially, releasing those translators whom the FBI must keep locked in basements all over Quantico to render their wiretap results useful to English-speaking agents. Once, concerning preventive detention of "terrorists"—they were also called Puerto Rican separatist criminals, freedom fighters, whatever you like—awaiting trial in Hartford for conspiring to commit politically-motivated bank robberies, the United States Government explained that two or three years of preventive detention was necessary while the wiretap evidence was translated from Spanish to English.[2] The process would have been much facilitated if it could have been made a crime to speak Spanish while engaged in making telecommunications for the purpose of planning crimes. Unfortunately for the poor policeman such a statute is facially unconstitutional. A mere "official English statute," requiring you to speak English not among yourselves, but with government only, is in all likelihood unconstitutional, let alone a regulation forcing use of a particular language in private conversation for the convenience of eavesdropping spooks.

Litigation of the official English issue, in the event that another such statute is unwisely enacted by a state legislature and a proper case is presented to the Supreme Court, would be a stepping-stone to the constitutional recognition of the freedom to speak PGP. At present, the discussion, when it happens at all, is dominated by foolish arguments against our right to choose our language—including a private or secret language—that will not stand the test of precise definition. Accordingly, they are presented imprecisely, and are hard to respond to.

First, it is said, secret speech is merely mechanical in its nature. I'm not exactly sure whether that's a criticism of my Serbo-Croatian or my PGP, but fundamentally after all, they are the same—modes of communication

[2] *See* United States v. Melendez–Carrion, 790 F.2d 984, 1006 (Feinberg, J. concurring).

chosen for their utility in a particular social setting, in which the motive to be comprehensible to some and incomprehensible to others is the same as that which lies behind many linguistic phenomena, such as the argot of teenagers, the jargon of post-structuralists, and the acronyms of bureaucrats. The level of technical intermediation between me and my listener is entirely irrelevant, utterly without First Amendment significance, as you are well aware.

Certainly, it can be declared, as it is in present regulations with respect to ham radio communications, that I may not use some particular segment of the government-administered public-trust airwaves for encrypted communications. And I won't at the present moment address the question whether, once we establish the root proposition that encrypted speech is protected, particular time, place and manner restrictions on the encrypted use of the airwaves in particular frequencies might withstand challenge. Where we reserve places (including spectrum locations) for speech to the public, it may be reasonable to ask that speech occur in comprehensible ways. But could one constitutionally prohibit amateur-frequency communication in Basque?

In any event, technical intermediation is not a ground of distinction. The media of communication useful with "natural" languages all may be used for encrypted language. They may be employed in writing or printing, by exchanges of telecommunications in fax or email, or the exchange of vocalized speech live through the network. And if some natural languages, such as sign languages, are difficult to employ in some technical settings, in absolute darkness for example, that does not make it constitutional to control their use.

Or else it is asserted, with particular foolishness, that PGP is not a "natural" language unlike, say, Sumerian. Certainly, you will object, Sumerian is an isolate with no ascertainable history, unused by anyone for thousands of years. But if I encrypt data by turning it into compressed transliterated Sumerian, for some "PGP isn't natural" objectors, that should alter the constitutional analysis. Meanwhile, the status of Esperanto and Gregg shorthand becomes just one of those little mysteries to be disspelled by hand-waving. When it comes, however, to the private languages often invented by identical twins and objects of durable interest to sociolinguists, where we are undoubtedly observing a cipher in use between confederates, the zealots of the distinction between natural and artificial languages have nothing left to do but attend the funeral of a theory killed by a fact, leaving us to get on with the real work.

The real work, then, begins in the recognition that PGP is as much a language as Navajo from the First Amendment perspective. Neither the involvement of a computer in its transmission nor the fact that like all language, "natural" or "artificial," it is an artifact of human intelligence changes our right to choose to speak it. Precisely because our choice to employ a language comprehensible to some and incomprehensible to others expresses our political, social, and personal intentions as well as the manifest content of particular speech acts, no system of free expression can tinker with our right to choose one language over another without risking fundamental commitments that the system itself values.

So linguistic regulation in our culture cannot be subjected to mere niggling as-applied challenges. For the reason usually advanced for extended rules of standing in First Amendment cases, the "chilling effect" (which is known, when cherished for its positive value by criminal law theorists, as "general deterrence") of constraining language choice makes it entirely unsuitable in our multinational democracy. Here, unlike the other empires of our enlightened time, one may vote in a language other than the dominant one, and States have an obligation to make such ballots available where their refusal unduly burdens political choice. For reasons so basic that they can await no demonstration of particular individual harm—and which brook no justification on the grounds that the speaker is a bad person—rules forbidding use of Navajo, French, Pittman, Esperanto and PGP are facially unconstitutional.

But, the police comedian rejoins, we're not seeking to forbid use of PGP, though we entirely reject the First Amendment argument on grounds we can't put clearly because the evidence is classified. We just want you to use our favorite form of escrowed encryption. No, no, not that form of French—use the one we understand! Even if that means a back door in the world financial system. Even if that means when in Iraq you have to escrow your keys with his secret police. Or else that the international escrow agents have to honor his subpoenas. For the policemen, the latter isn't a problem, while for the spook that would be unquestionably destructive.

In fact the whole conversation, however promisingly full of ripe and fruity controversy between realists and rights-mongers, is futile. As I shall show in a moment, strong unescrowed end-to-end encryption of the net is available and is here to stay. Technology does affect policy, to reassure a couple of other participants this afternoon, who have suggested some doubt on the subject. The printing press affected policy, and so has the movement for free strong encryption software.

Others are indeed right to claim that government regulation futile in the long run is not therefore unconstitutional in the present. Government may take a step at a time even in directions potentially nugatory. What is unconstitutional about encryption regulation of any blanket kind—mandatory escrow, outright bans, maximum key lengths, forbidden algorithms, forcibly classified research, and so on—has nothing to do with factual futility.

But that doesn't make futility unimportant. Because futility is an outgrowth of individual choice, and is therefore a consequence of democratic choice. Which is where you come in.

When people discuss encryption controls, they normally do so as though what needed to be controlled were the algorithms used and the lengths of the keys. "Strong" encryption means good algorithms using large keys. So strong encryption is what some of us want people not to use. Here, at this small point, is another source of conflict between the policemen and the spooks. The spooks, concerned with the content of communications and unconcerned with their admissibility in court, want weaker encryption or keys that are easy to steal. Police, for whom large-scale code-breaking is economically out of reach and whose evidence must be admissible in the end, want someplace to serve a warrant or a subpoena.

But neither their agreement nor their disagreement is as important as what they do not discuss at all. What really makes their activities futile in the end is explosive increase in the volume of encrypted material. Today, the global communications system operates almost completely in the clear; the bulk of secret communication is small enough to allow the spooks to concentrate all their pitiful attention on it. Because almost all communications activity is cleartext, very little of it is anonymous, so wiretaps and subpoenas for particular phone lines will mostly get the policeman what he wants. But if you all decide to turn the net into an encrypted medium, globally, their methods of operation, both spook and cop, become almost utterly worthless.

Let us take the poor, bereft spooks first. The American Empire has been built since mid-Cold War on our power to intercept all the telecommunications of our friends, our enemies, and everyone else.[3] This purpose has required harnessing enormous and profoundly expensive quantities of computing power. But the power necessarily grows linearly with the volume of communications for which its services are necessary. If encrypted traffic

[3] Except, of course, US nationals living in the United States, on whom they never, never, never....

on the net were to grow from less than 1% of the total to 100% of the total (what we would call an end-to-end encrypted network), NSA would need to increase that portion of its budget by two orders of magnitude, which is out of the question, or immediately improve, without additional capital expense, analytical computation by two orders of magnitude more than required to keep pace with basic improvements in cryptography, which is unlikely.

For the policemen, too, the lot of the listener in an end-to-end secure net is not a happy one. Although current network design—which considers anonymity an unimportant property and actively works against it—would not be fundamentally altered, anonymity would be practically possible whenever desired, as it will be all the time by people who wish to evade policemen. They too will lose in the actual new world.

But is an end-to-end encrypted net inevitable? After all, the design of Internet 2 has been hung up on this issue for years, thanks to export controls and the deliberate obscurantism of the government agencies that present ghostly reverberating versions of NSA positions. But again, as with PGP, the free software world has provided the answer. The whole goal of those of us who have been seeking both technically and legally to secure unregulated and unregulatable encryption since the beginning of the 1990s was to bring about the time when the network would be widely and strongly encrypted—in which the volume of encryption would have passed the point at which it could be reversed. I am here to tell you, despite the rather pessimistic statistics you have heard today, that the time is here already. I use a supposedly-obsolete 133MHz notebook computer; I bought it for $800. It is, from anyplace in the world where there is a twisted pair of copper wire, a secure telephone. It also uses the program called Secure Shell, SSH, that makes end-to-end encrypted connections with other computers all over the network. SSH is available free to anyone who wants it. A commercial version is even available for people who use Microbrain software.[4] Thus, equipped only with free software available to anybody on the planet and without any special hardware, a very cheap computer, apparently much inferior to ones you use yourself, can provide strongly encrypted voice and data communications, transparently and without appreciable performance loss, everywhere.

Thus the question of the technically possible is a settled question. The only issue is whether you all will decide you want to use it. If you de-

[4] Microsoft is a registered trademark. Microbrain is a fact.

cide to make yourself part of the net's encrypted traffic, that completes the revolution and the discussion is over. The spooks and the cops will have to get used to the brave new world, and while they will complain about it, and warn themselves silly about the terrible consequences of a freedom you cannot resist, those of us who know the difference between what *is* true and what we *wish* were true will move on to other questions.

Of course, if the futility of regulation depends on individuals' choice to be part of the process, then the outcome—like all democratic outcomes—remains in doubt. I'm betting on you. Your power to change the world depends solely upon what, in a democracy, is basic: that we ensure you not merely the right to vote, but also the right to express yourself. A right valued by civilized man and dangerous to tyrants only. Ah, but the policemen are not tyrants. Quite right, they're not. They are not tyrants until, like King Canute, they decide they can command the ocean, at which point a better definition of tyranny cannot be afforded you.

So there you have it: you're the ocean. They will command you or they won't. The choice will be yours. I think you've a First Amendment right to choose. I expect to carry that First Amendment right, when the time is ripe—which is not in these piddling little cases we are presently having—into the Supreme Court and I expect to see it there soundly vindicated at enormous apparent social cost. But you must not allow the estimation of the cost to be conducted in the way that the policemen estimated for you: "Ah, we shall have this and this and this nuclear terrorism, we shall have that and that and that pedophilia." This form of calculation is very scary, but it is fundamentally and flagrantly wrong. A truly encrypted network, a secure telecommunications environment embracing the whole planet, prevents more crimes than it causes. It prevents all the financial fraud that is inevitable in a world of back-doored financial communications, where he who steals the keys steals everything.

It also prevents fingernails being ripped out, not to mention worse things being done, by nasty people all over the world who have a tendency to tap telephones and torture people based on what they hear. When the television center at Vilnius was under attack by Soviet troops in 1991 one of the beta testers of PGP, a native of an adjacent Baltic republic, wrote to Phil Zimmerman, "You know, it may be that the old times are coming back again. But now we'll have PGP." At the present moment, in northern Thailand, people whom we call "freedom fighters," and whom Myanmar's SLORC regards as terrorists subverting true justice and order, are learning to use PGP on cheap laptops. They are securing the communications infrastructure of the revolution that will eventually free Burma. Now, you can regard all that as totally unimportant; the crimes of political repression elsewhere are not your problem. Your problem is just money laundering by cocaine dealers in Miami. But in the world of the net you must take a more global picture than that. You must remember that the policemen you are disappointing are not just our good policemen but also other people's quite evil policemen who commit crimes too. And when you remove from them the possibility of committing those crimes, you are preventing a lot of evil.

So we must see that the balance we strike when we destroy all control over encryption is rather more complicated than the policemen let on when they talk about the crimes they would not have prevented without wiretapping. It is also about the crimes we will prevent when people may speak freely, everywhere, all the time. The good that will come from that is hard to overestimate. But the constitutional environment is quite simple. And, as I said at the beginning, though you might not have been able to understand it in the language I was using at the time, there's really nothing very new to say just because the methods of communication are new. The methods of communication are new, but the principles—in whatever language you express them, and it's your choice—are very familiar indeed.

I don't doubt that there will be downsides. You should accept the truth that harms will be caused, as harms are caused by free speech all the time. But don't let yourself be panicked about this. The world of the twenty-first century will be more free, and will continue to be, as the spooks often say, "a tough neighborhood." Indeed, some bombs will go off; there will be, in Stewart Baker's signature phrase, "some mangled, burnt bodies." You will notice that there are already. But fewer of them will be in Iraqi prisons; none of them will ever again be in a gulag or Lager maintained by a KGB or SS state with a tap on every telephone. And of that you should be very proud, because it is we who will have made it possible.