

# Publicity, Privacy, and Permanence of Information

Charles H. Bennett

*IBM Research, POB 218, Yorktown Heights, NY 10598, USA*

**Abstract.** The quantum principles of superposition and entanglement have led to a recasting of the foundations of information and computation theory, and are especially helpful in understanding the nature of privacy. The most private information, exemplified by a quantum eraser experiment, is best regarded as existing only conditionally and temporarily—after the experiment is over no trace remains. Less private is classically-secret information—quantum information that has decohered, and thus become recoverable in principle, though not in practice, from portions of the environment. Finally there is public information, which has been replicated so thoroughly throughout the environment as to be infeasible to conceal. The Internet has caused an explosion of public information, with the beneficial side effect of making it harder for despots to rewrite the history of their misdeeds, and it is tempting to hope that all macroscopic information is permanent, making such cover-ups impossible in principle if not in practice. However, by comparing entropy flows into and out of the Earth with estimates of the planet's storage capacity, we conclude that most macroscopic information—for example the pattern of sand grains on an ancient beach—is impermanent, in the sense of becoming irrecoverable in principle from the Earth though still recorded in the Universe.

**Keywords:** quantum, classical, macroscopic, information, erasure, public, private

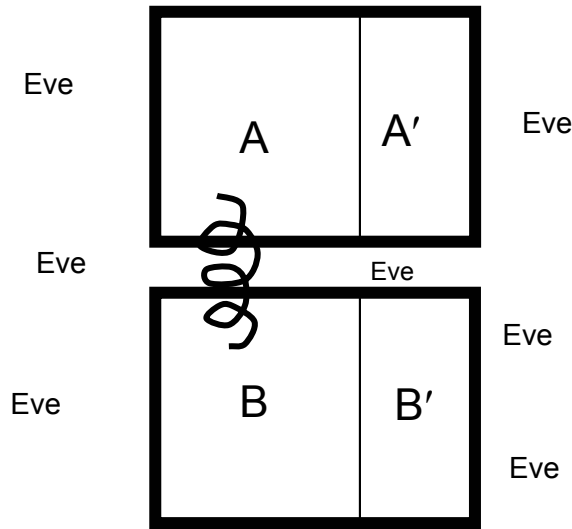
**PACS:** 01.70.+w, 03.67.-a, 89.70+c

Ordinary classical information, such as the information in a book, has a solid existence independent of the observer. By contrast quantum information, for example the polarization of a single photon, is fragile and private, more like the information in a dream. Many people can read a book and get the same message, but trying to tell people about your dream changes your memory of it, so that eventually you forget the dream and remember only what you said about it. Along with fragility comes privacy: you cannot prove to someone else what you dreamed, and you can lie about your dream without getting caught. Another dreamlike feature of quantum information, not unconnected with fragility and privacy, is evanescence, or what might better be called its tentative ontological status. In a cliché of crime fiction, the soft-hearted perpetrator, instead of killing his witnesses, tells them “This never happened!” in the hope that they will return his kindness by not telling the police. In the quantum world, the passage of a particle through one of two slits, or in principle anything that has “happened,” can subsequently be undone, indeed made never to have happened, by a sufficiently careful quantum erasure procedure. Unlike classical undos, for example replacing something you were about to steal before anyone notices it's

missing, quantum erasure erases all memory of the undone deed—one can fairly say that even God has forgotten.

The fragility of quantum information finds practical application in cryptography, in the art of quantum key distribution [1]. Some QKD protocols are based on the preparation, transmission, and measurement of non-orthogonal quantum states with subsequent discussion over a public classical channel. Others use the quantum and public channels respectively to share and verify the possession of a high quality entangled state, then locally measure it to produce correlated secret random bits. The security in this case rests on the so-called monogamy of entanglement, the fact that two parties maximally entangled with each other are necessarily in a product state with the rest of the universe, including any potential eavesdropper.

Suppose two parties, conventionally called “Alice” and “Bob”, initially share a maximally entangled bipartite state  $\Psi^{AB}$  of two particles A and B and then measure it locally, each in their own laboratory, to generate a bit of shared secret key. The key only remains secret in principle as long as the Alice and Bob can keep their adversary “Eve” out of their local environments  $A'$  and  $B'$ , respectively representing parts of Alice’s and Bob’s laboratories which interact with the entangled particles in performing the measurement.



**FIGURE 1.** An entangled state (helix) is converted into a shared secret key by local measurements, but the key remains secret only so long as Alice and Bob can keep their local environments  $A'$  and  $B'$  away from their adversary Eve.

Conversely, standard prepare-and-measure key distribution protocols, when carried out coherently with the help of local environments well insulated from Eve, become protocols for entanglement sharing. Private local environments can even help make secret key from non-distillable mixed states [2]. To do so, Alice and Bob make local measurements on the mixed state  $\rho^{AB}$  (which may be viewed pessimistically as a pure tripartite state  $\Psi^{ABE}$  of Alice, Bob and Eve) but hold onto local environments  $A'$  and  $B'$  which, if they fell into Eve’s hands, would compromise the key.

In practice, the more macroscopically a key is stored, the more difficult it will be to keep it out of Eve's hands. In principle, as soon as a secret key bit is recorded in any macroscopic medium like paper or a hard disk, it will begin to rapidly decohere relative to the environment outside their lab, just as Schrödinger's cat decoheres even before its box is opened.

Among various theories of decoherence and the onset of classicality, the notion of "quantum Darwinism"[3] identifies classical information as that which is redundantly replicated throughout many parts of the environment. In this view, a system's classical properties are those that are *public*, in the sense that many independent observers, each having access only to part of the environment, would agree as to their value.

We can thus tentatively distinguish three levels of privacy of information (see the end of this article for a more refined version of the hierarchy),

- **Quantum:** Information, like the path of a particle through an interferometer or quantum eraser experiment, that exists only temporarily and afterward is best thought of as never having existed.
- **Classically Private:** Information that has been amplified and propagated to the point of becoming classical, and can be recovered in principle, but not in practice. Humans can erase it, and then lie about it with impunity, although perhaps not without guilt. As technology improves, and is exploited by journalists, historians, and archaeologists, information can move from this level to the next.
- **Public:** Information that exists in many redundant copies and is known by many people. Lying about such information only makes the liar look foolish.

The Internet has greatly increased the scope of public information and made it harder to retract. Websites have been set up with the purpose of keeping once-public information available when, as often happens, its originators later find it embarrassing and try to suppress it. In the practical tradeoff between publicity and privacy, digital technology has created a problem and an opportunity: Cheap, easy-to-use video cameras and cheap data storage lead to the temptation to record everything happening in public or even private places and save it forever, with ensuing loss of privacy, and potentially a loss of liberty if a latter-day J. Edgar Hoover [4] gets hold of the data and uses it to harass citizens for holding the wrong political beliefs. But these recordings, aside from deterring crime, can also protect human rights and promote the rule of law, as in the case of Rodney King in Los Angeles, whose beating by police was recorded by an amateur videographer [5]. The organization Witness.org aims to discourage rights abuses by placing video cameras in the hands of amateurs likely to witness them.

A peculiar viewpoint prevalent in the US is that society benefits when everyone has the right to carry a gun. A more sensible idea would be for everyone to carry a camera. Public policy would encourage amateurs to make audiovisual recordings, while restricting how the recordings can be used (Yes for exposing crime and corruption; no for blackmail). A recent advertising billboard in Delhi, by the news company CNN, captured this idea concisely in the slogan, "If you see it, shoot it—every citizen a

photojournalist,” although their motivation may be to gather juicy news stories of all sorts, rather than specifically to deter wrongdoing.

In view of all this capacity for recording and publicity, it is tempting to believe that in the modern world, information that has once become public can never be destroyed. The modern world is quite different in this regard from the pre-Gutenberg era, when major literary works were written down, performed, and widely known, but then lost. An extreme case is Sappho’s poetry, of which Martin West [6] reported last year,

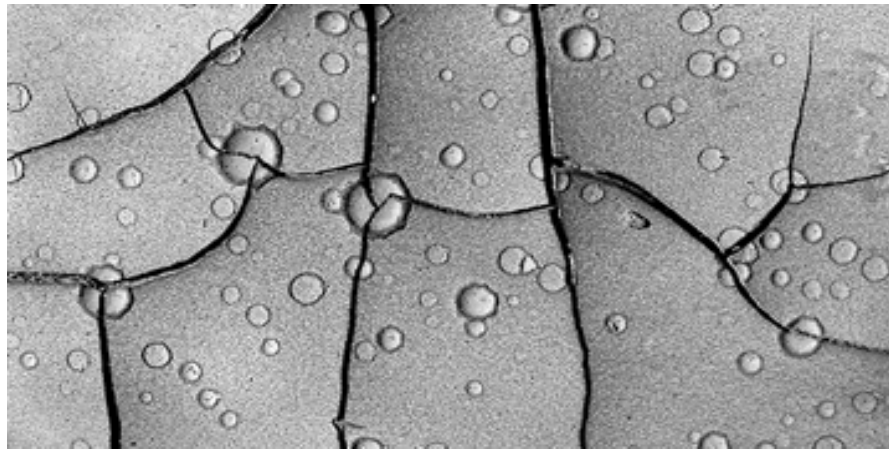
*“The ancients, who had nine books of her poems at their disposal, were unstinting in their admiration.... It is difficult to judge her for ourselves when so little of her work remains. What we have consists on the one hand of quotations and more general references in ancient authors, and on the other hand of torn scraps from ancient papyrus and parchment copies.... Only twenty-one contain any complete stanzas; and only three – till now – gave us poems near enough complete to appreciate as literary structures.*

*“A recent find enables us to raise this number to four... This text, recovered from Egyptian mummy cartonnage, is the earliest manuscript of her work so far known. It was copied early in the third century bc, not much more than 300 years after she wrote.”*

A perhaps even more poignant example, from this subcontinent, suggested by Soumya Chakravarti of the University of California at Berkeley, is the Carvaka school of philosophy, prevalent from about 600 BC- 1400 AD, but now known mainly from fragments of its texts quoted by its Hindu and Buddhist opponents [7].

Another kind of possibly lost information is the fate of persons like Jimmy Hoffa, who disappeared in 1975 under suspicious circumstances but whose body has never been found, though police are still looking for it [8].

I will argue that even today, much macroscopic, publicly accessible information is lost because no one considers it worth remembering, and no natural process happens to record it in a durable medium (cf. Fig. 2).



**FIGURE 2.** A photograph of raindrop marks in drying mud in a river bed in Las Vegas, USA in 1965. A few days later these cracks and craters were washed away by a subsequent rain. If they had not been photographed, would they have remained recoverable in principle from other terrestrial information?

Still it is tempting to believe that such macroscopic information is not lost, just that it becomes so diffusely and complexly spread out as to be irrecoverable in practice but not in principle. A popular way of putting this is that physical processes are reversible, so when a book is burned, its contents should be recoverable in principle from the state of the smoke and ashes. Can it be that every major past phenomenon, say Sappho's poems, or the fate of Jimmy Hoffa, is recoverable from physical evidence, in principle if not in practice? To believe otherwise is to venture dangerously close to the deconstructionist view, abhorred by most scientists, that history is not what "actually" happened, merely what we believe to have happened.

I will argue nevertheless that much macroscopic information really is lost, not from the universe, but from the world—the planet Earth—because of the earth's large fluxes of entropy into it from the sun and out of it in the form of thermal radiation. Returning to the book-burning example, to say that the book's contents are recoverable from its smoke and ashes ignores another combustion product—heat, in the form of photons of emitted radiation, which would need to be captured and saved to reverse the burning process. But many typically escape the earth soon after combustion.

The radiative input and output power of the earth are approximately in balance at a few hundred watts per square meter of the earth's surface, corresponding to an entropy input of around  $10^{29}$  bits per square meter per year. The entropy output at first would seem to be about an order of magnitude greater, because of the isotropy of the outgoing radiation and its lower temperature; but one can argue (because the earth's entropy is not changing very much) that the outgoing radiation is less random than it appears, being significantly entangled with itself.

Neglecting the relatively poorly understood mantle and core, the quantitatively most important medium for long term terrestrial information storage is probably frozen-in atomic-scale disorder in rock of the earth's crust. Crudely estimating its information storage density in as 1 bit per cubic nanometer, the crust thickness as 10 km, and the typical lifetime of rock between formation and remelting in subduction zones as  $10^8$  years, one obtains a possible information capture rate around  $10^{22}$  bits per square meter per year, much smaller than the gross entropy fluxes into and out of the earth.

One can also estimate the human information capture rate in digital media, say 1 billion heavy information users at around 100 gigabyte per user per year, giving around  $10^{21}$  bits, which looks quite respectable until one recalls that that is for the whole world, not per square meter.

But suppose some future civilization, whether as an instrument of tyranny or out of an obsession with irrelevant details of its past and a distaste for deconstructionism, tried to place the whole of the earth's surface under continuous video surveillance, say at millimeter-millisecond resolution, and store the result in rock—would there be enough capacity to do so? Yes; it is easy to estimate that such surveillance would generate "only" about  $10^{16}$  bits of data per square meter per year, comfortably less than the geological storage capacity estimated above.

We don't have that sort of purposeful surveillance, but is it possible that the earth's dynamics, without any help from human engineering, is already efficiently storing local macroscopic information—the kind that would be revealed by millimeter-scale

surveillance? Clearly some such information is stored, for example in the form of fossils and more generally sedimentary processes of all sorts, including seafloor ooze, glacial ice, and alluvial deposition. But it is likely that much more classical information is lost, in the manner of the burned book, when dynamical processes transform it to an unstable form, allowing essential parts of it to escape the earth.

Consider the life history of a typical piece of macroscopic information, say the location where a raindrop hits the ground. The information will have originated by amplification of microscopic thermal and quantum fluctuations during the drop's formation and fall. However, by the time the drop lands, perhaps making a crater as in Fig. 2, the information is thoroughly classical. The drop does not fall in a superposition of places, and many independent observers would agree as to where it fell. More concretely, as long as the drop or its crater persists, reflected sunlight or starlight will deliver a more or less intense torrent of redundant replicas of the information to diverse parts of the environment, satisfying the quantum Darwinist criterion of classicality (this optical replication process would occur even if the illuminating radiation were thermal. This may at first appear paradoxical because, as is well known, thermal radiation inside a blackbody cavity carries no information about the objects it illuminates. However any mixed state, such as thermal radiation, may be regarded as arising from an ensemble of pure states known to some preparer, or as a subsystem of some larger system in a pure entangled state. In either case, the state of the larger system, including the preparer or the purifying reference system, is affected when the thermal radiation scatters off objects in the cavity.).

If, as usually happens, the crater is not stabilized by incorporation into a sedimentary rock formation, nor its image captured in a photograph, the formerly unambiguous classical information of the raindrop's impact location will lose any stable macroscopic embodiment, as the crater is washed away in a subsequent rain. The water molecules formerly constituting the raindrop, and the sand grains formerly constituting the crater, will be dispersed to multiple locations, in a complicated way depending on new thermal and quantum fluctuations, and some of the information required to reconstruct their history will be radiated into space. Meanwhile the photons comprising the torrent of optical replicas of the former crater will undergo their own complicated evolution, being absorbed, reflected, and also partly lost into space.

How much information about the input to a complex dynamical evolution can be inferred from partial information about its output? This of course depends on the evolution, but a simple model of such processes is a known but random permutation  $\mathbf{P}$  on bit strings of length  $N$  bits (the quantum analog would be a known but random unitary transformation  $U$  on a Hilbert space of dimension  $2^N$ ) in which  $k \ll N$  bits of macroscopic information interact with a larger number  $N-k$  of random bits representing microscopic information, e.g. fresh quantum and thermal fluctuations. After the interaction, the microscopic part of the output,  $N-k$  bits, is lost, e.g. in the form of escaped radiation, while the remaining  $k$  bits, representing the macroscopic part of the output, are examined in an attempt to infer the macroscopic part of the input. In both the classical and quantum cases, only an exponentially small (in  $N-2k$ ) fraction of a bit about the macroscopic part of the input can be inferred from knowledge of  $\mathbf{P}$  (resp.  $U$ ) and the macroscopic part of the output.

We thus arrive at a revised hierarchy with a new level, Classical but Escaped:

- **Quantum:** Information, like the path of a particle through an interferometer or quantum eraser experiment, that exists only temporarily and afterward is best thought of as never having existed.
- **Classical but Escaped:** Information that, after having been amplified to the point of becoming classical, has escaped from earth, so that it is now irrecoverable in principle from terrestrial sources, even though it still exists in the universe.
- **Classically Private:** Information that has been amplified and propagated to the point of becoming classical, but exists in only a few stable terrestrial copies (each generating a torrent of redundant, escaping replicas). By definition this information is not widely known, and if the few stable copies were all lost or destroyed, the information would become classical-but-escaped.
- **Public:** Information that exists in so many and so widely distributed stable terrestrial copies that it is infeasible to find and destroy all of them. If not already widely known, such information can be discovered and by definition is infeasible to suppress.

The last two levels are here redefined less anthropocentrically, in terms of the number and distribution of terrestrial copies, rather than how many people know. “Public” information would now include the history of geomagnetic field reversals, which being redundantly recorded in rocks all over the earth is quite infeasible to expunge, unlike, say the whereabouts of Jimmy Hoffa’s body. In Sappho’s time no one knew about geomagnetic field reversals, and yet they proved more durable than her poetry. Perhaps the Gutenberg/Internet information revolution has finally succeeded in giving human cultural creations, or the best of them, the kind of earthly immortality they deserve.

## ACKNOWLEDGMENTS

I thank John Smolin and Aram Harrow for helpful discussions.

## REFERENCES

1. M. Dusek, N.Lütkenaus and M. Hendrych “Quantum Cryptography” to appear in *Progress in Optics* **49**, eprint quant-ph/0601207.
2. Karol Horodecki, Debbie Leung, Hoi-Kwong Lo, Jonathan Oppenheim, *Phys. Rev. Lett.* **96**, 070501 (2006), eprint quant-ph/0510067
3. Robin Blume-Kohout, W.H. Zurek, “Quantum Darwinism: entanglement, branches, and the emergent classicality of redundantly stored quantum information,” (subm. to *Phys. Rev. A.*) quant-ph/0505031.
4. See for example [http://en.wikipedia.org/wiki/J.\\_Edgar\\_Hoover](http://en.wikipedia.org/wiki/J._Edgar_Hoover)
5. Rodney King <http://news.bbc.co.uk/2/hi/americas/2119943.stm>
6. Martin West, Times (London) Literary Supplement, 24 June 2005.
7. See for example <http://en.wikipedia.org/wiki/Carvaka>
8. See <http://news.bbc.co.uk/2/hi/americas/4993016.stm>