HTCIA Membership Rules:
A Debate

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Computer Information Systems
School of Business & Management
Norwich University, Northfield VT

The High Tech Crime Investigation Association (HTCIA< http://www.htcia.org/ > is a respected organization to which I belonged until 2003, when I felt I had to resign according to the bylaws. The story – and a debate about HTCIA membership rules – comes out in a correspondence with Duncan Monkhouse< http://ca.linkedin.com/pub/duncan-monkhouse/2/900/966 >, President of the HTCIA for 2011. Mr Monkhouse has very kindly agreed to publish our correspondence.

Mich Kabay to HTCIA:

Dear Colleagues,

I was an enthusiastic member of the HTCIA until I was hired by parents to investigate an accusation of unauthorized system access against their son at a private school. My investigation showed that the accusation was based on incorrect information and the case was dropped. I wrote about the situation as follows to a colleague in December 2003:

> *5) No member by virtue of their employment be in a position to represent or assist the defense in a criminal prosecution.*

Belonging to an organization that prevents its members from "assisting the defense" is morally repugnant to me and should be a source of shame and embarrassment to the entire organization. It seems to me that the administration of justice in a society of laws depends absolutely on the impartial sharing of evidence *and expertise* with both prosecution and defense.

I urge the HTCIA membership to rethink their stand on this exclusionary rule.

In any case, I am certainly excluded from membership in the HTCIA, since my position as a professor and consultant makes me perfectly capable (and willing) to serve justice by aiding either the prosecution or the defense as required. This notice will serve as my resignation from the HTCIA effective immediately. I will be taking down the framed membership plaque from my wall with sincere regrets and will particularly miss the HTCIA list.<

Recently I received an announcement about a student poster competition sponsored by the HTCIA and I went to your site to see if conditions have changed. They have, but not for the better.

I looked at the current description of the HTCI < http://www.htcia.org/htcia_code.shtml >:

> ***HTCIA Code of Ethics***
>
> *I will support the objectives and purposes of the HTCIA, as stated in Article II of the Association Bylaws.*

I agree to respect the confidential nature of any sensitive information, procedures, or techniques that I become aware of because of my involvement with the HTCIA.

I will not disclose such confidential material to anyone who is not a member in good standing of the HTCIA without the written permission from the HTCIA Board of Directors.

HTCIA Core Values

(1) The HTCIA values the Truth uncovered within digital information and the effective techniques used to uncover that Truth, so that no one is wrongfully convicted!

(2) The HTCIA values the Security of our society and its citizens through the enforcement of our laws and the protection of our infrastructure and economies.

(3) The HTCIA values the Integrity of its members and the evidence they expose through common investigative and computer forensic best practices including specialized techniques used to gather digital evidence.

(4) The HTCIA values the Trusted network of forensic and investigative professionals within private and public businesses including law enforcement who share our values and our vision.

(5) The HTCIA values the Confidentiality of its membership and the information, skills and techniques they share within the association.

Then I looked at the Bylaws < http://www.htcia.org/bylaws.shtml >. This clause stands out for me:

5) Members may not, by virtue of their employment be in a position to represent or assist the defense in a criminal prosecution, unless < list of conditions >....

How do you reconcile Core Values (1) and Bylaws (5)?

* * *

Duncan Monkhouse, President, HTCIA:

Professor Kabay,

Thank you for your email concerning the HTCIA code of ethics and bylaws. The sections that you drew my attention to were from the code of ethics:

The HTCIA values the Truth uncovered within digital information and the effective techniques used to uncover that Truth, so that no one is wrongly convicted!

and from the bylaws:

Members may not, by virtue of their employment be in a position to represent or assist the defense in a criminal prosecution, unless ...

You asked how HTCIA could reconcile the two, given the standard of impartiality to which reputable forensic examiners adhere. Our response is threefold:

First, the requirement of HTCIA members not to assist the defense is one that has been brought forward a number of times in recent years. Because of this, the bylaw section relating to defense work has been modified in some significant ways. These include allowing membership for court-appointed forensic examiners, as is the situation in the United States military and in some foreign countries. We also allow an HTCIA member to work for the defense, if the work is pro bono and the member receives chapter approval, or if the member is subpoenaed by the court.

That said, we ask the community to remember that HTCIA membership comprises a wide range of investigators in many roles, not just digital forensic examiners. We understand the argument that bringing together investigators for the prosecution and the defense promotes higher standards of evidence-gathering and thus due process. However, we do not believe that the current criminal legal system, which is adversarial by design, allows for the free exchange of information between those investigators. In a similar manner, I would not expect a defensive player to be allowed into the offensive huddle in a football game. All the players have the same goal of playing their best. But that does not allow for collaboration between opposing players on the field.

Finally, the goal of all investigators, forensic and otherwise, is to uncover the truth. To assist the people investigating high tech crimes, HTCIA provides a wide variety of training: an International Training Conference and Expo, regional conferences, and local Chapter meetings. We do not usually restrict who can attend the training.

HTCIA encourages its members to attend any relevant training from any source, including defense expert witnesses. HTCIA hopes that by providing the best possible training to the investigators of high tech crime that they are positioned to uncover the truth, to the best of their ability, and will thereby be able to present correct findings to prosecutors.

I hope that this has clarified HTCIA's position on our code of ethics and bylaws. If you have any further questions or comments please feel free to contact me.

* * *

Mich Kabay to Duncan Monkhouse:

Dear Mr Monkhouse,

Thank you for your courteous and complete reply.

You wrote, "However, we do not believe that the current criminal legal system, which is adversarial by design, allows for the free exchange of information between those investigators. In a similar manner, I would not expect a defensive player to be allowed into the offensive huddle in a football game. All the players have the same goal of playing their best. But that does not allow for collaboration between opposing players on the field."

There is no question of collaboration on the specifics of a particular court case; just as you explain, the members of the opposing teams must not collude in preparing evidence.

However, there should be no question that all forensic investigators *must* benefit from the scientific, technical and methodological advances of our field. I would never forbid sports aficionados from discussing what kind of new footwear or shielding could improve performance and safety; would you and other members of the HTCIA advise against such information sharing? When a colleague publishes a

scholarly paper on the use of, say, EEG waves in an improved lie-detector, would you seriously propose that investigators should hide the information from others based on whether their principal roles are for defense and prosecution?

Would you approve of a technical security association in which anyone who works on penetration testing is to be excluded from membership because most of the members work on configuring intrusion prevention?

To me, the notion that contributing to defense efforts versus prosecution efforts defines two different categories of experts is an abomination. Defense and prosecution are *roles*, not defining attributes of a professional. A professional is not "infected" or "tainted" by working for the defense on contract; your own rules make it clear that the *only* factor determining exclusion is that a professional work for *fees* for the defense.

If it is necessary for members of the HTCIA to discuss a *specific* and *ongoing* legal case, that should be done outside the HTCIA under full control of applicable laws –- otherwise there could be legal consequences. Otherwise, however, I see no benefit whatsoever in excluding members who happen to work for a defense team on contract.

I helped a defense team in a case involving gross negligence and incompetence in chain of evidence and chain of custody when a child was accused of criminal hacking in a school; that contract forced me to resign from the HTCIA. But my analysis saved a kid from prosecution based on an unjust accusation. Do I regret taking the case? Absolutely not. Do I regret that I had to leave the HTCIA? Sure – as you can see from my taking the time to argue with you even though I resigned in 2003!

* * *

Duncan Monkhouse to Mich Kabay

Thank you for providing me with your opinion on the matter of allowing people who work for the defense into HTCIA.

This is a thorny issue with many excellent arguments on each side. We do not disagree that "all forensic investigators *must* benefit from the scientific, technical and methodological advances of our field." This is why we do not, as mentioned, restrict defense experts from attending our training sessions, including our International Conference; we do not ask that our sponsors, or vendors do not aid or train the defense experts; and we do not prevent our members from sharing information with defense experts. We believe that these measures satisfy our core value of Truth as well as our bylaw requirement.

We have asked our membership a couple of times in the last few years about allowing defense experts to enroll as members, and the response has always been to maintain the status quo. We believe that this is largely because our investigator members come from many walks besides law enforcement and legal. They include regulatory agencies, corporate investigators and counsel, brand protection experts and auditors. They come from a variety of sectors including telecommunications, aerospace, utilities, transportation, manufacturing and food production, among others. Their work may involve some degree of digital forensics, but also includes intelligence-gathering, scientific research and old-fashioned legwork.

Thus many of our members are not comfortable with the presence of experts whose job it is to find reasonable doubt. In the course of due process, it is common for investigators to have questions about a particular tool or procedure they have not encountered before. We do not believe that any investigator

would deny the importance of a continuous learning process, but would not want that learning to be introduced as "doubt" that the investigator knows how to do his or her job. At no other point in the investigative process does a defense expert have pre-discovery access to the actions that compose due process, and we do not believe that we should provide it.

Again, we believe that our exclusions for military, foreign-country, pro-bono and other defense work more than adequately allow for the opposing side's perspective and experience, and we welcome the same perspective and experience at our training events.

Readers should feel free to respond to these ideas using the comment section of this blog.

* * *

Duncan Monkhouse< http://ca.linkedin.com/pub/duncan-monkhouse/2/900/966 > is President of the High Tech Crime Investigation Association (HTCIA< http://www.htcia.org/ >). He has been serving as Electronic Evidence Officer for the Government of Canada since since 2001 and was an IT Security Consultant for the Government of Canada for nine years before that. He has also been the Manager of Specialized Computer Training at the Canadian Police College.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >